OIPE JC84
SEP 27 2004
PATENT & TRADEMARK OFFICE

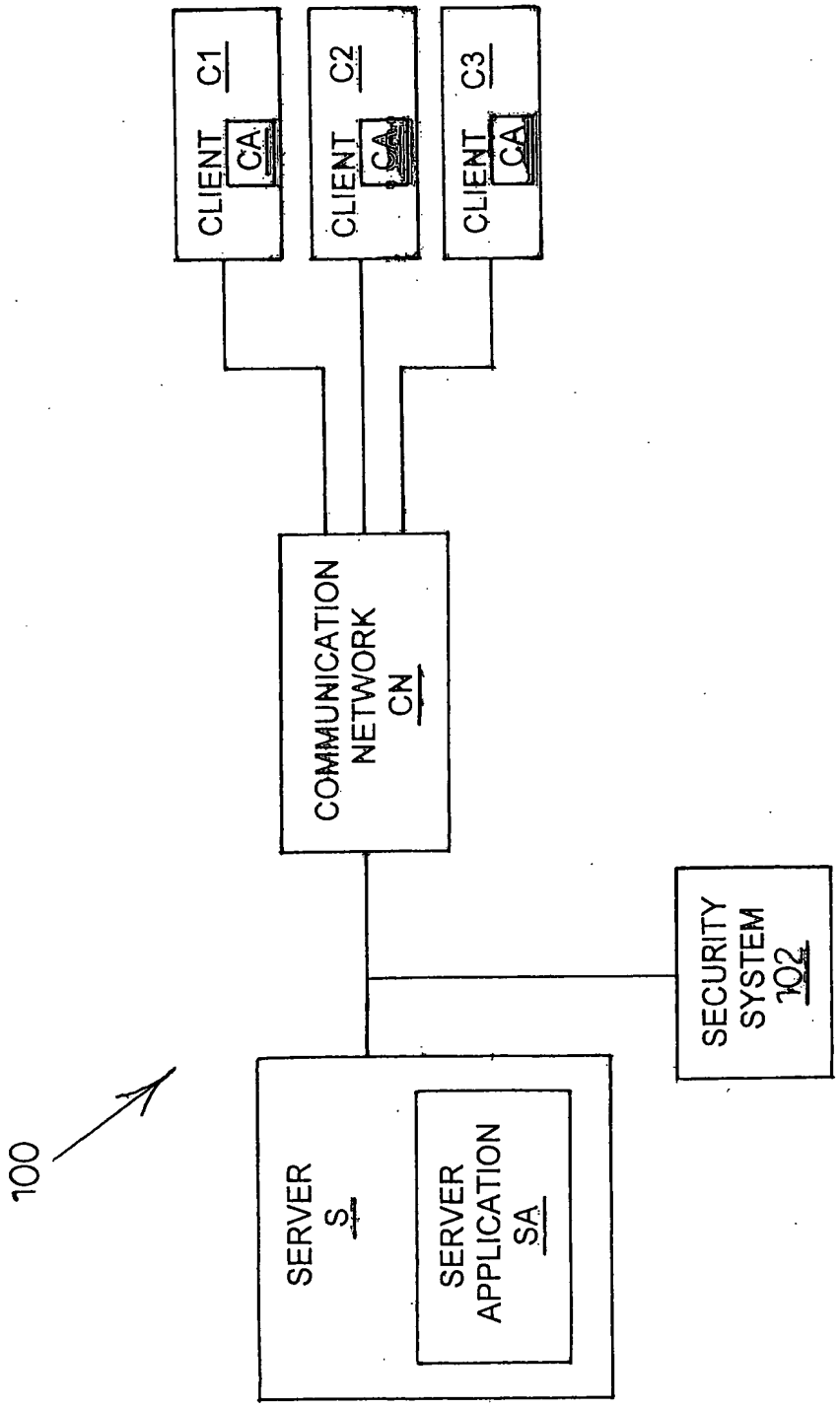

FIG. 1A

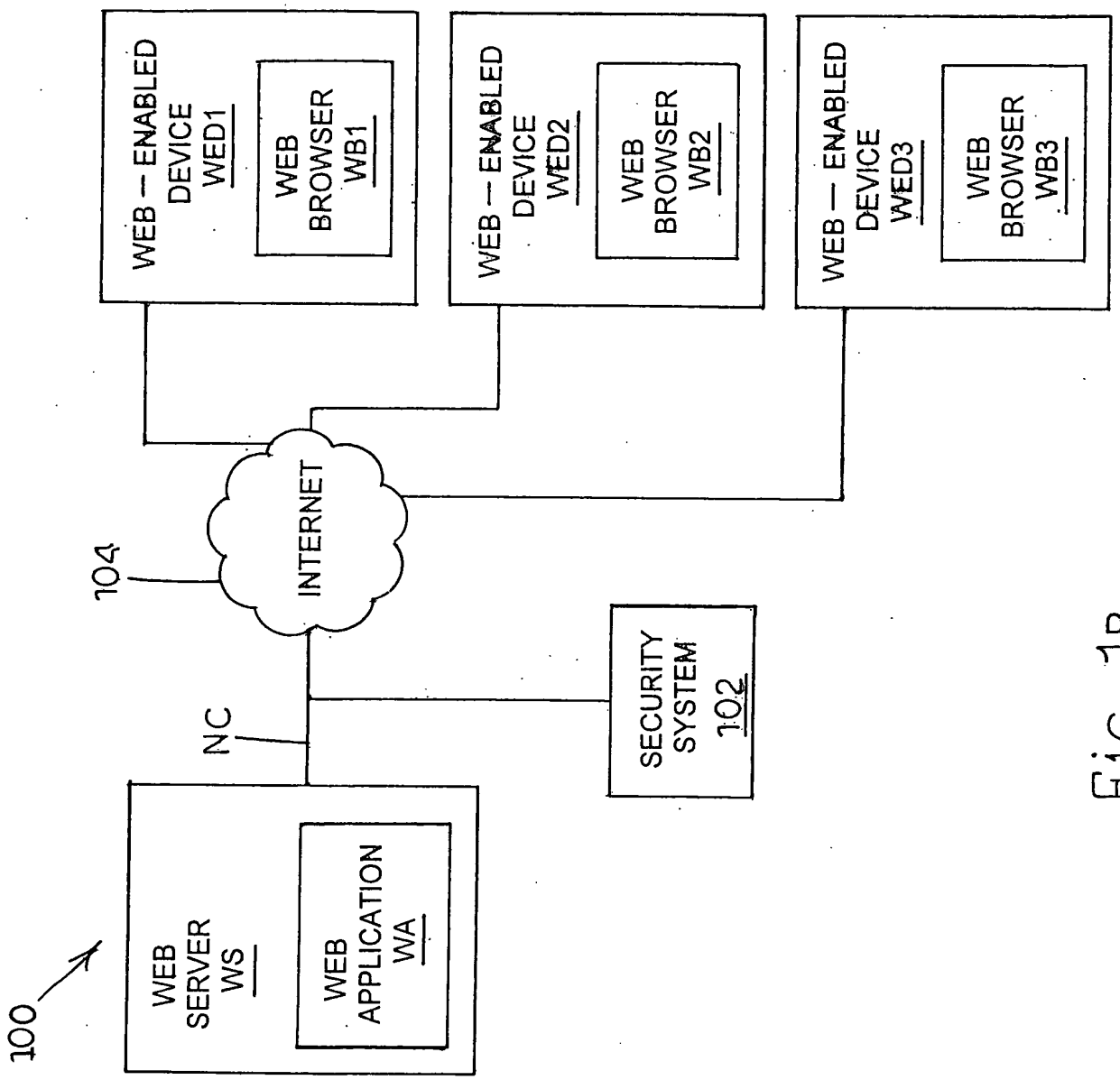
WEB – ENABLED DEVICE WED1
WEB BROWSER WB1
WEB – ENABLED DEVICE WED2
WEB BROWSER WB2
WEB – ENABLED DEVICE WED3
WEB BROWSER WB3
INTERNET
104
SECURITY SYSTEM 102
NC
WEB SERVER WS
WEB APPLICATION WA
100

FIG. 1B

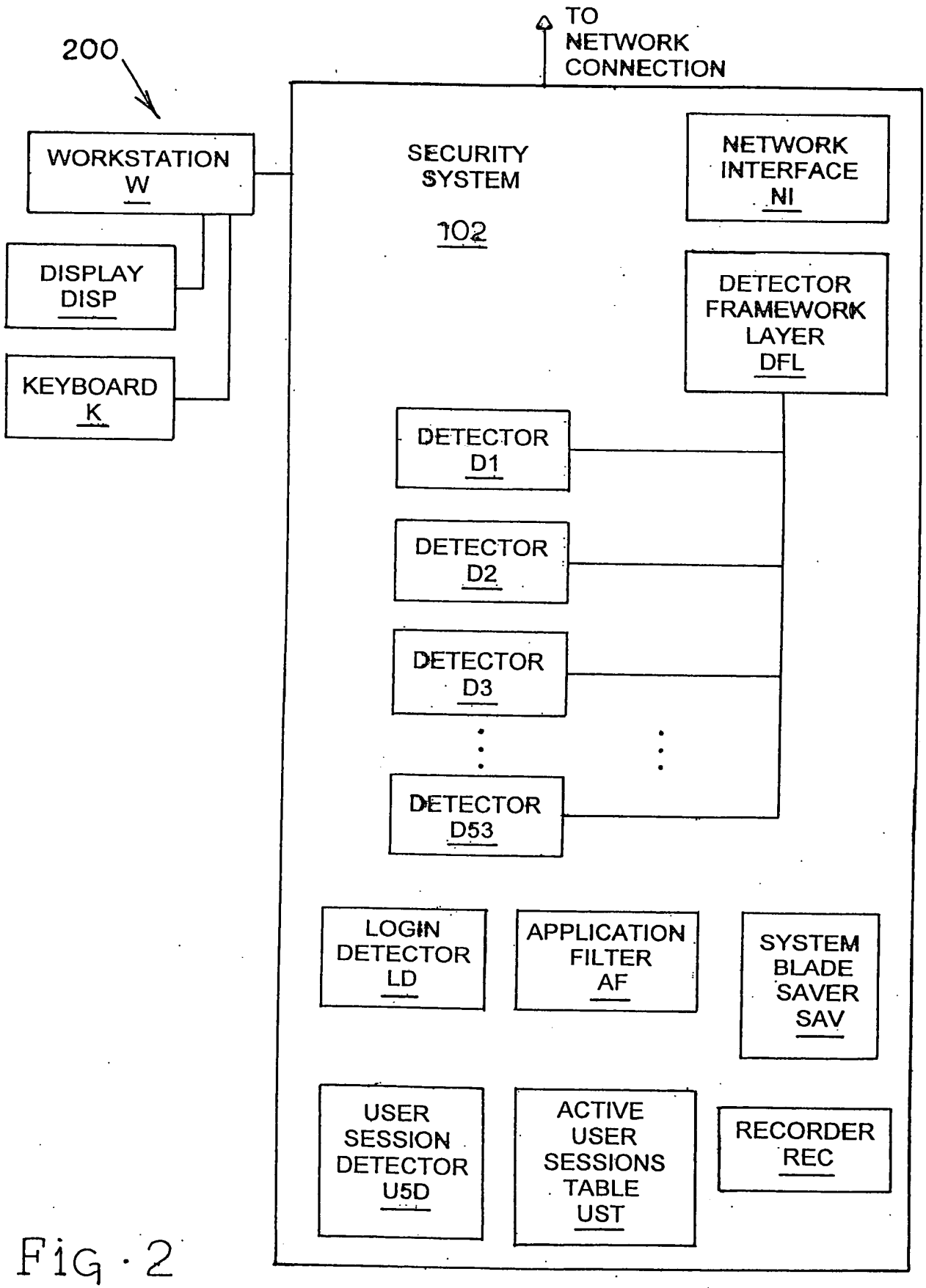
200
TO NETWORK CONNECTION
WORKSTATION W
DISPLAY DISP
KEYBOARD K
SECURITY SYSTEM 102
NETWORK INTERFACE NI
DETECTOR FRAMEWORK LAYER DFL
DETECTOR D1
DETECTOR D2
DETECTOR D3
DETECTOR D53
LOGIN DETECTOR LD
APPLICATION FILTER AF
SYSTEM BLADE SAVER SAV
USER SESSION DETECTOR U5D
ACTIVE USER SESSIONS TABLE UST
RECORDER REC

Fig. 2

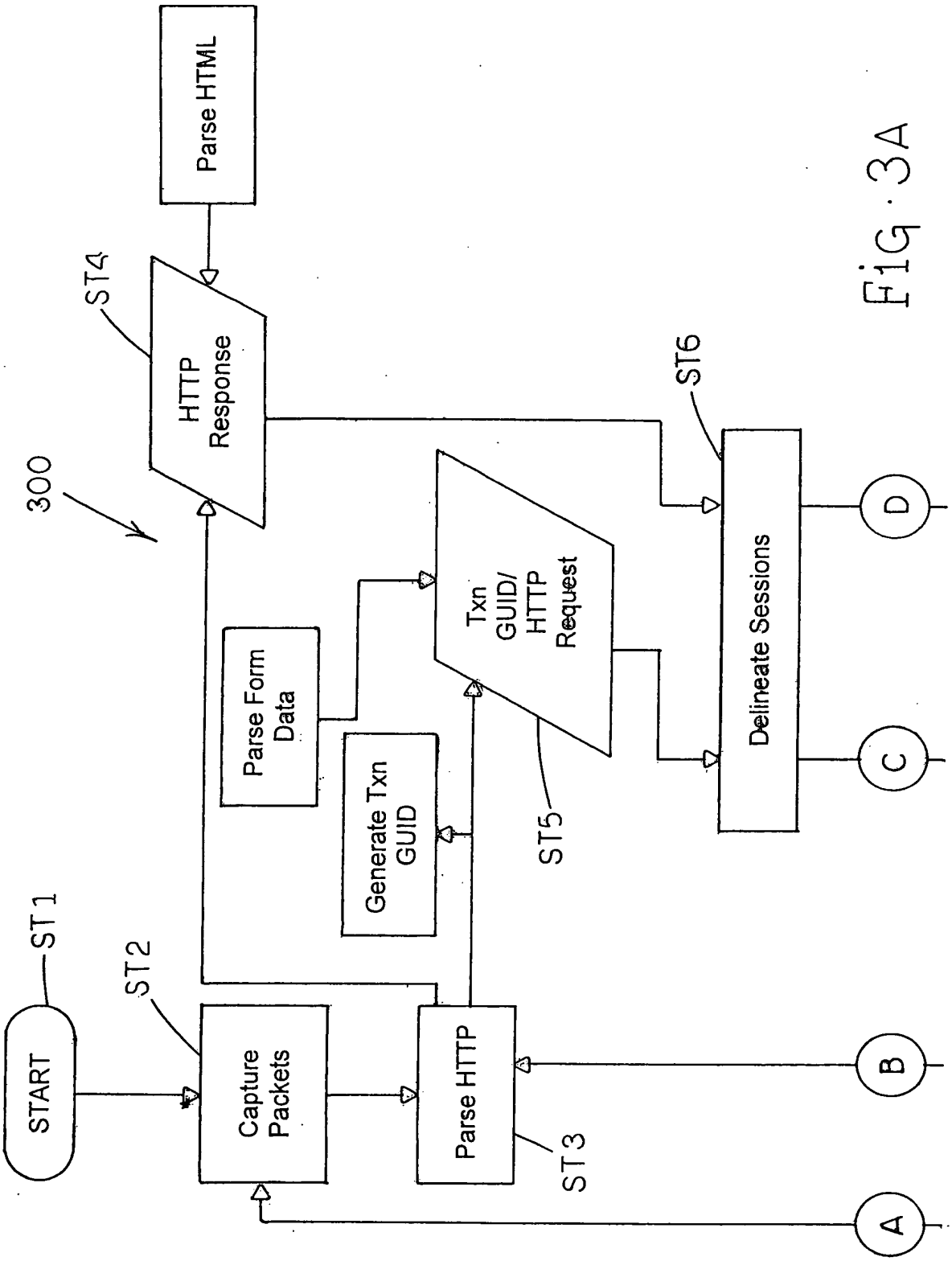
START
ST 1
Capture Packets
ST2
Parse HTTP
ST 3
Generate Txn GUID
Parse Form Data
Txn GUID/ HTTP Request
ST5
HTTP Response
ST4
Parse HTML
300
Delineate Sessions
ST6
A
B
C
D

Fig. 3A

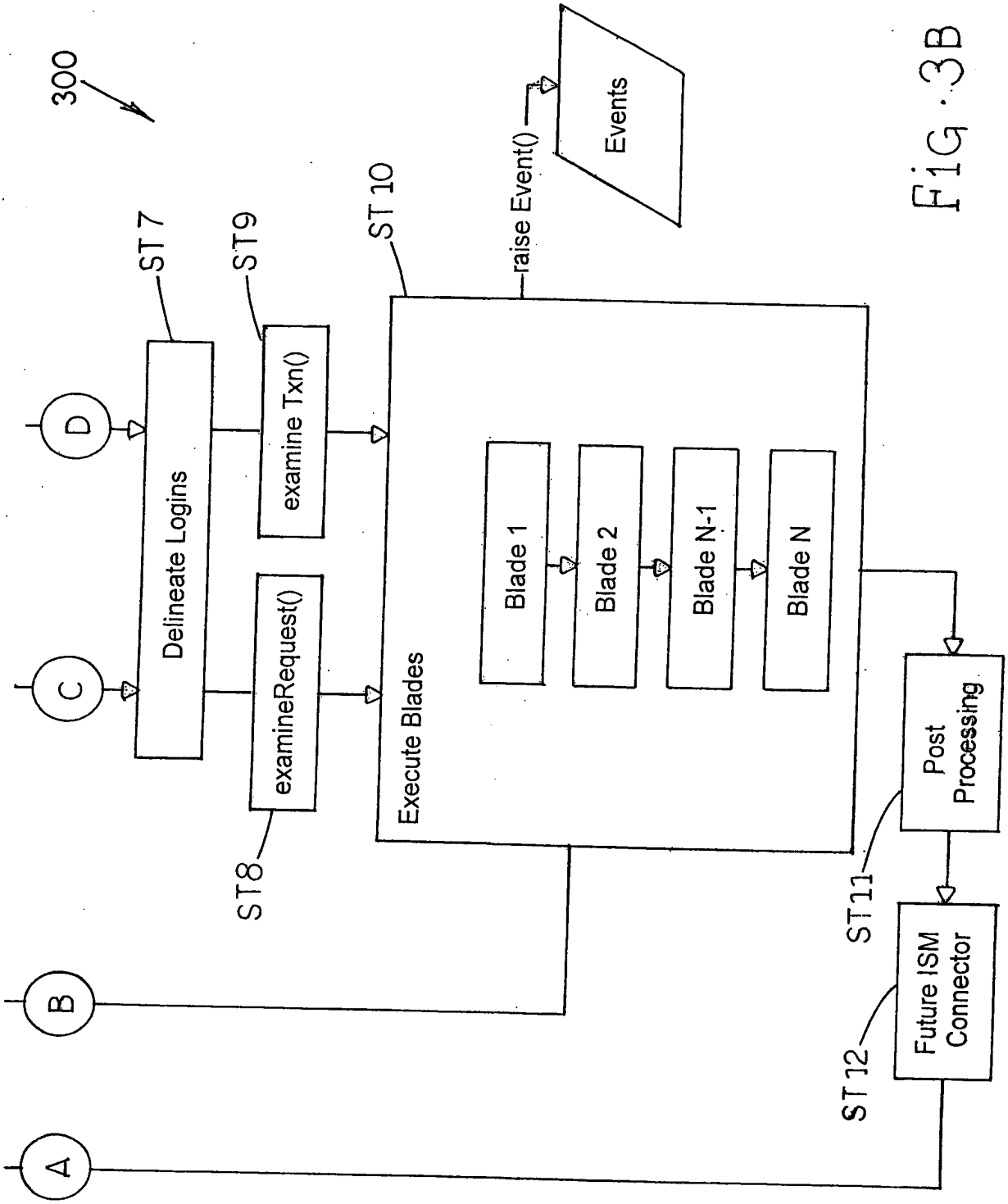
300
Events
raise Event()
ST 10
ST 7
ST9
D
Delineate Logins
examine Txn()
C
examineRequest()
ST8
Execute Blades
Blade 1
Blade 2
Blade N-1
Blade N
Post Processing
ST 11
Future ISM Connector
ST 12
B
A

FIG. 3B

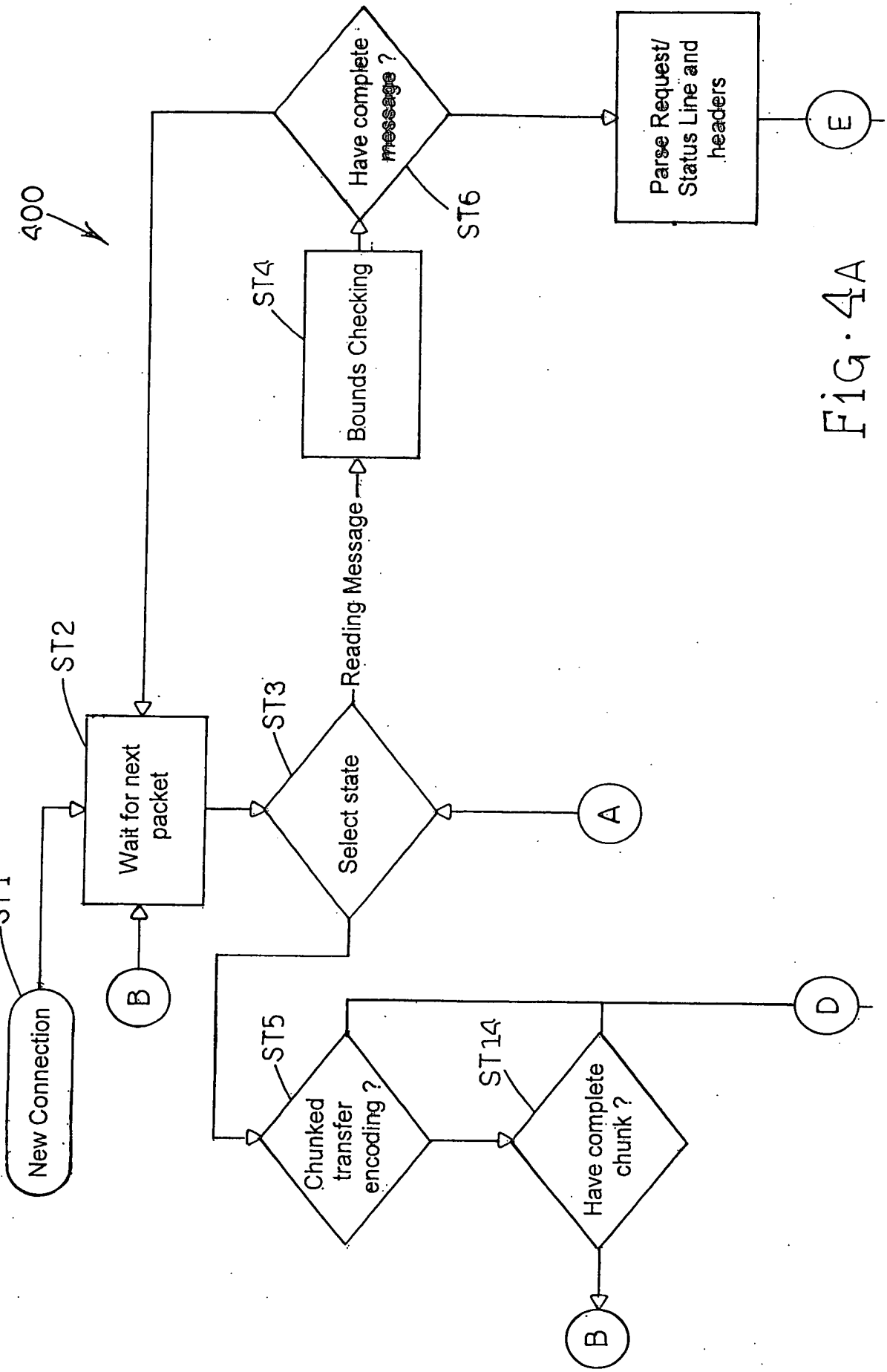
400
ST1
New Connection
ST2
Wait for next packet
B
ST3
Select state
Reading Message
A
ST4
Bounds Checking
ST5
Chunked transfer encoding ?
ST14
Have complete chunk ?
B
D
ST6
Have complete message ?
Parse Request/ Status Line and headers
E

FIG. 4A

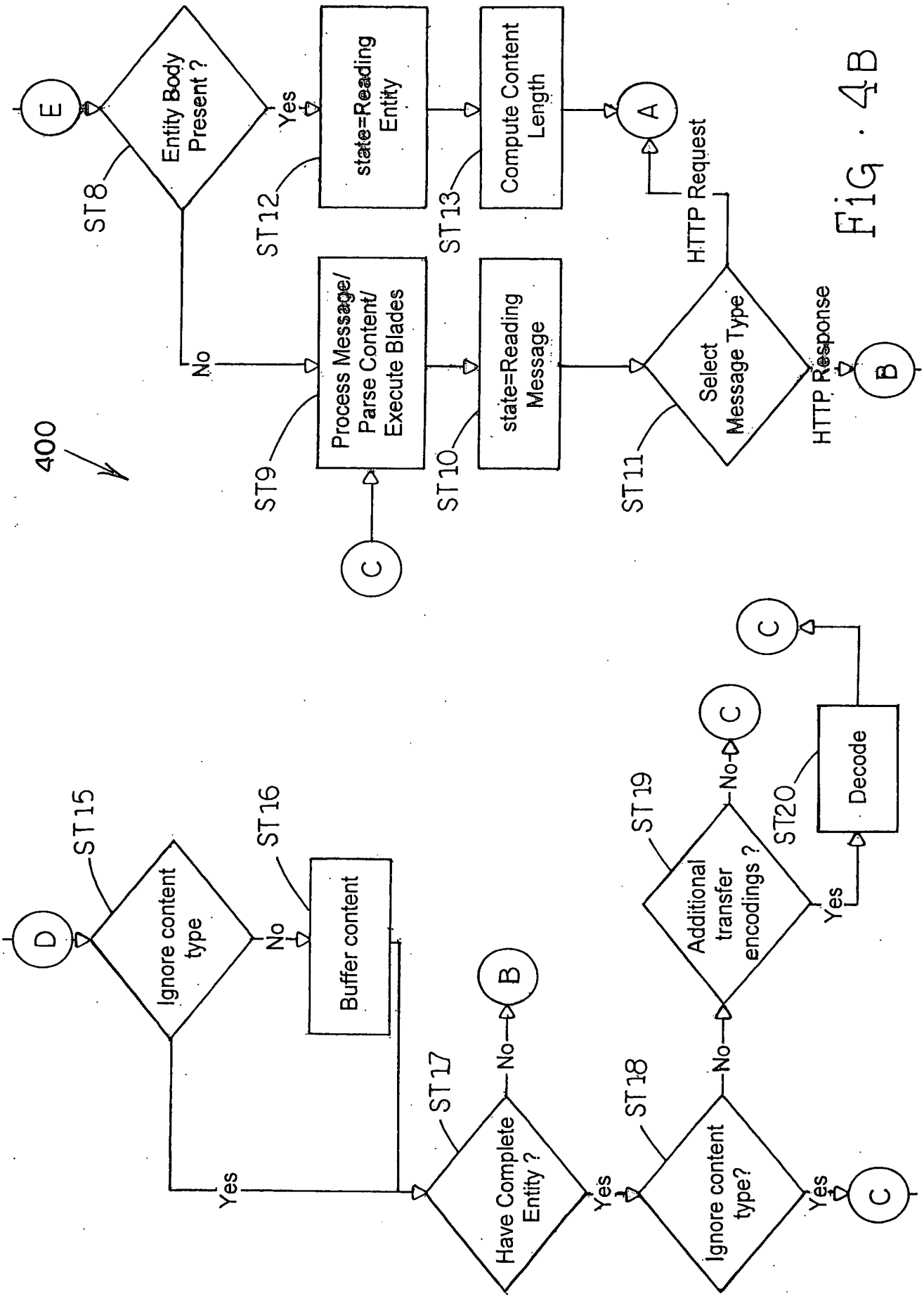
400
E
Entity Body Present ?
ST8
Yes
No
state=Reading Entity
ST12
Compute Content Length
ST13
A
HTTP Request
Process Message/ Parse Content/ Execute Blades
ST9
state=Reading Message
ST10
Select Message Type
ST11
HTTP Response
B
C
D
Ignore content type
ST15
No
Buffer content
ST16
Yes
Have Complete Entity ?
ST17
No
B
Yes
Ignore content type?
ST18
No
C
Yes
Additional transfer encodings ?
ST19
No
C
Yes
Decode
ST20
C

FIG. 4B

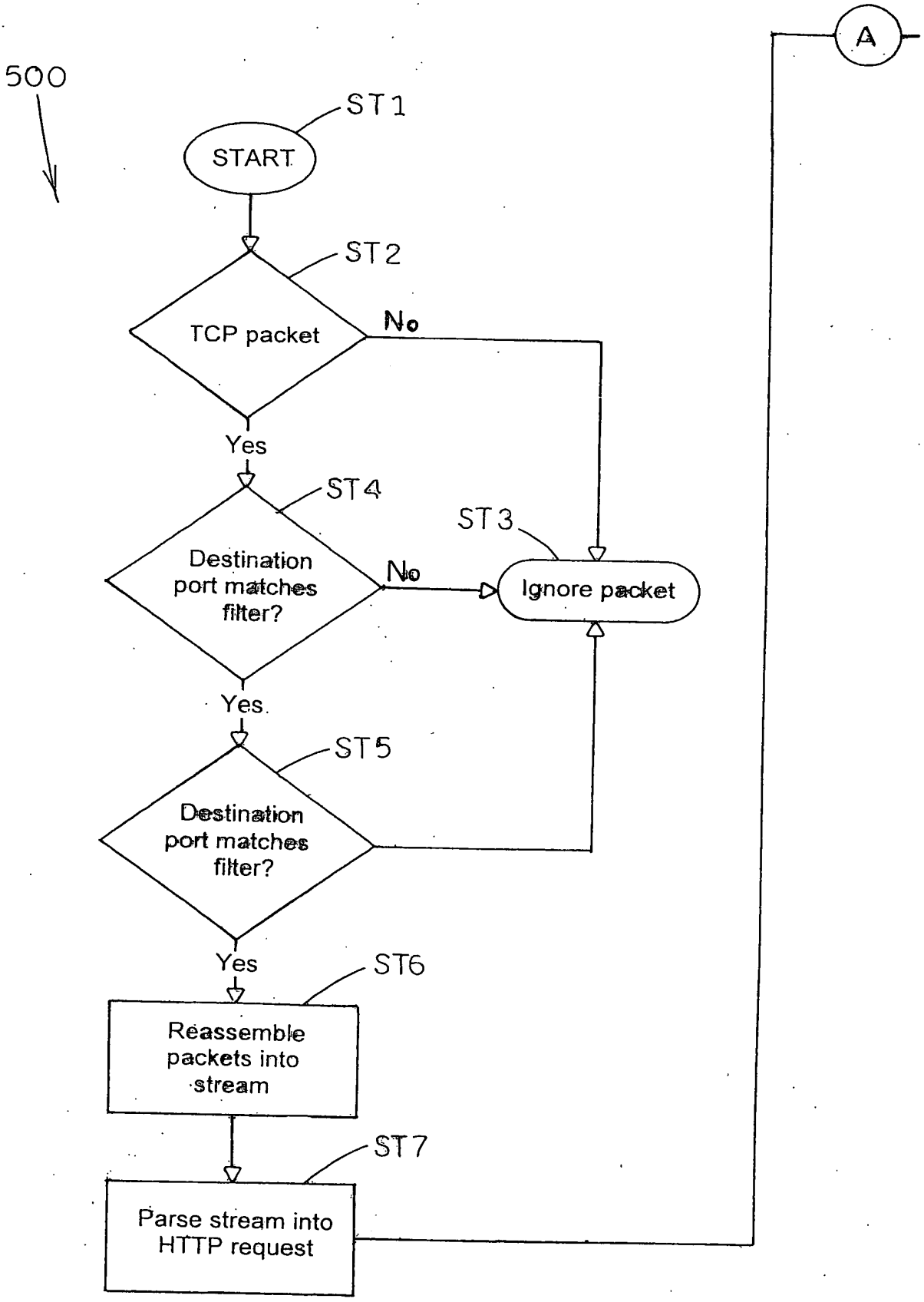
500
ST1
START
ST2
TCP packet
No
Yes
ST4
Destination port matches filter?
ST3
No
Ignore packet
Yes
ST5
Destination port matches filter?
Yes
ST6
Reassemble packets into stream
ST7
Parse stream into HTTP request
A

FIG. 5A

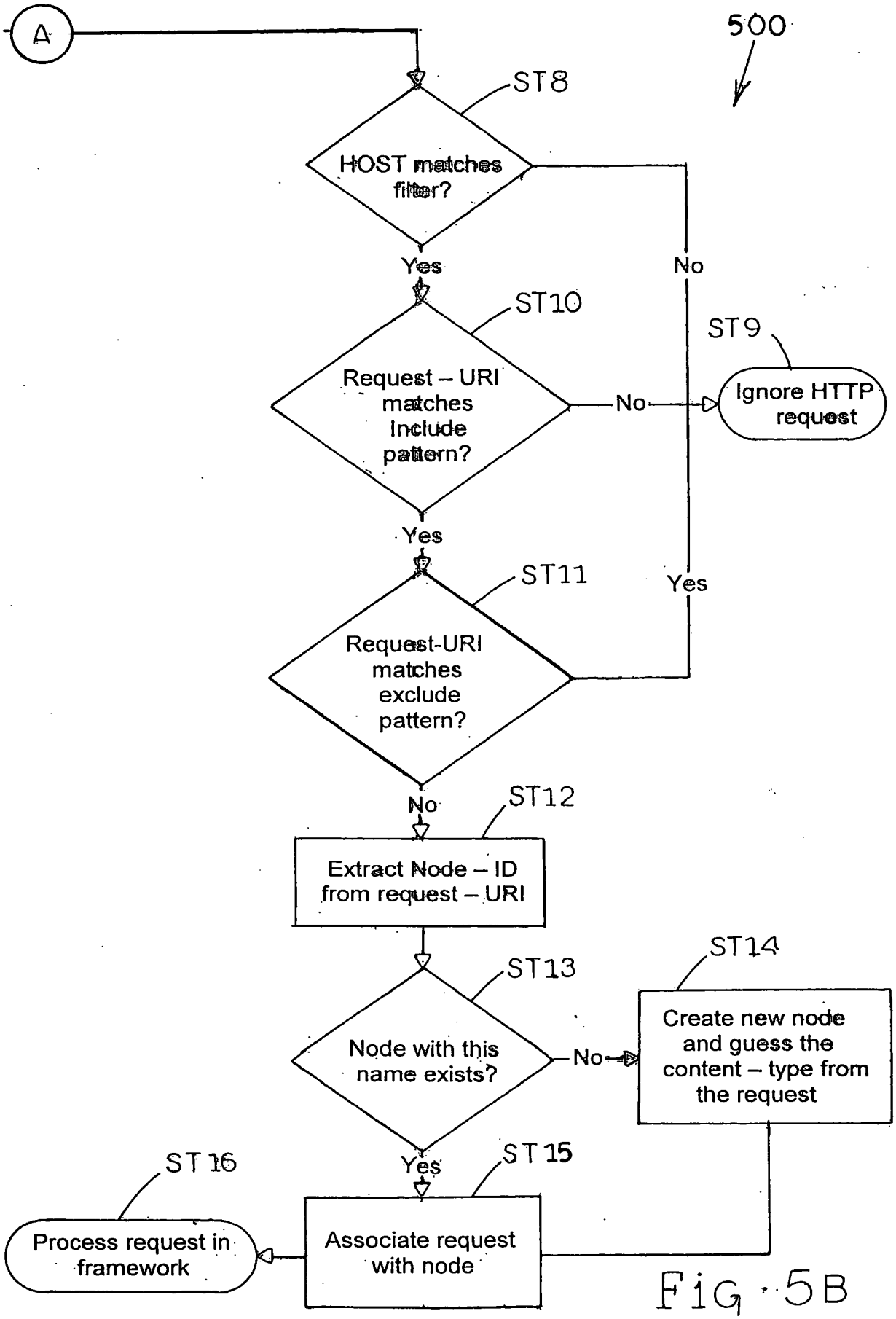
A
500
ST8
HOST matches filter?
Yes
No
ST10
Request – URI matches Include pattern?
No
ST9
Ignore HTTP request
Yes
ST11
Request-URI matches exclude pattern?
Yes
No
ST12
Extract Node – ID from request – URI
ST13
Node with this name exists?
No
ST14
Create new node and guess the content – type from the request
Yes
ST15
Associate request with node
ST16
Process request in framework

Fig. 5B

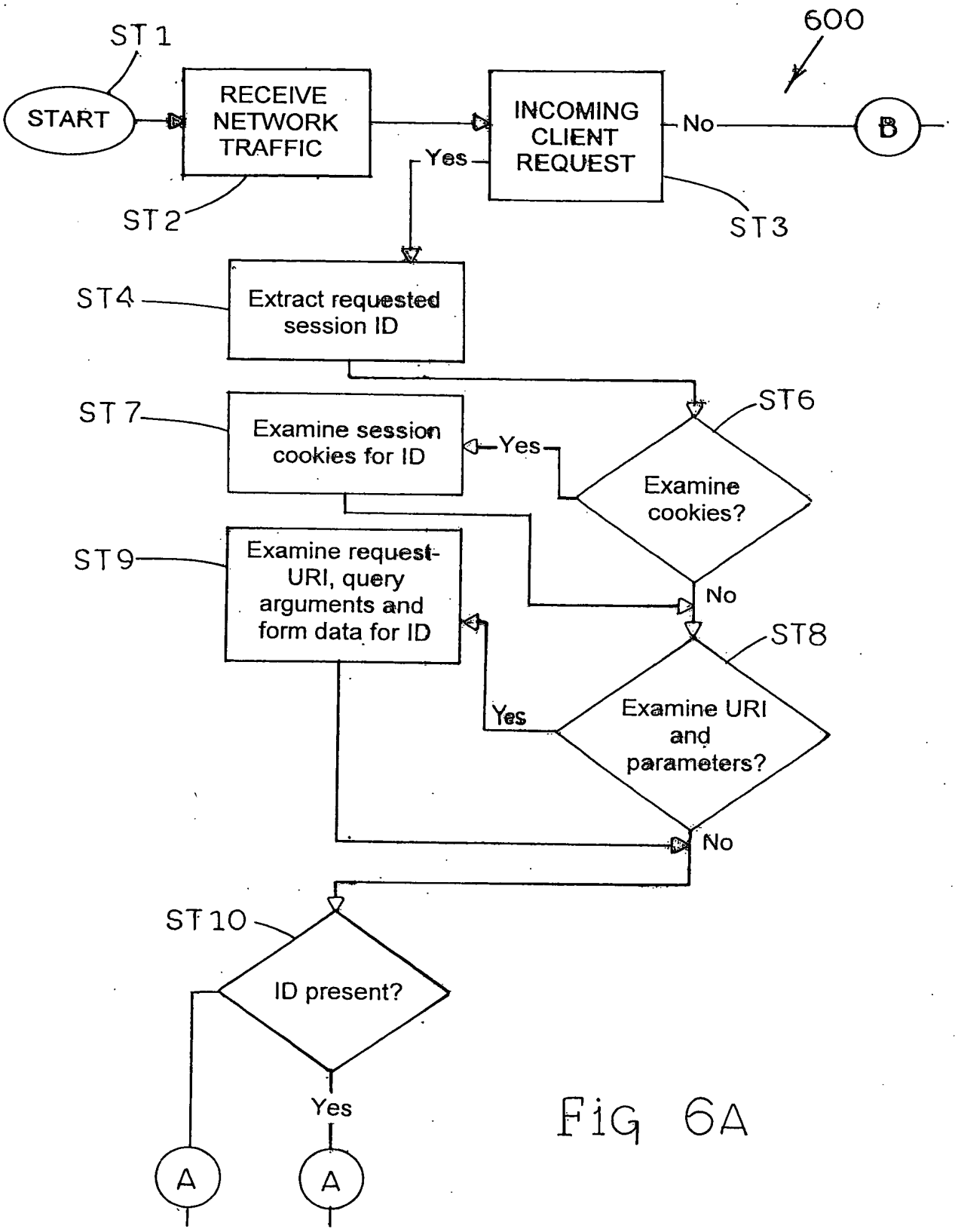
600
ST 1
START
RECEIVE NETWORK TRAFFIC
ST2
INCOMING CLIENT REQUEST
No
B
Yes
ST3
ST4
Extract requested session ID
ST 7
Examine session cookies for ID
Yes
ST6
Examine cookies?
ST9
Examine request-URI, query arguments and form data for ID
No
ST8
Yes
Examine URI and parameters?
No
ST 10
ID present?
Yes
A
A

Fig 6A

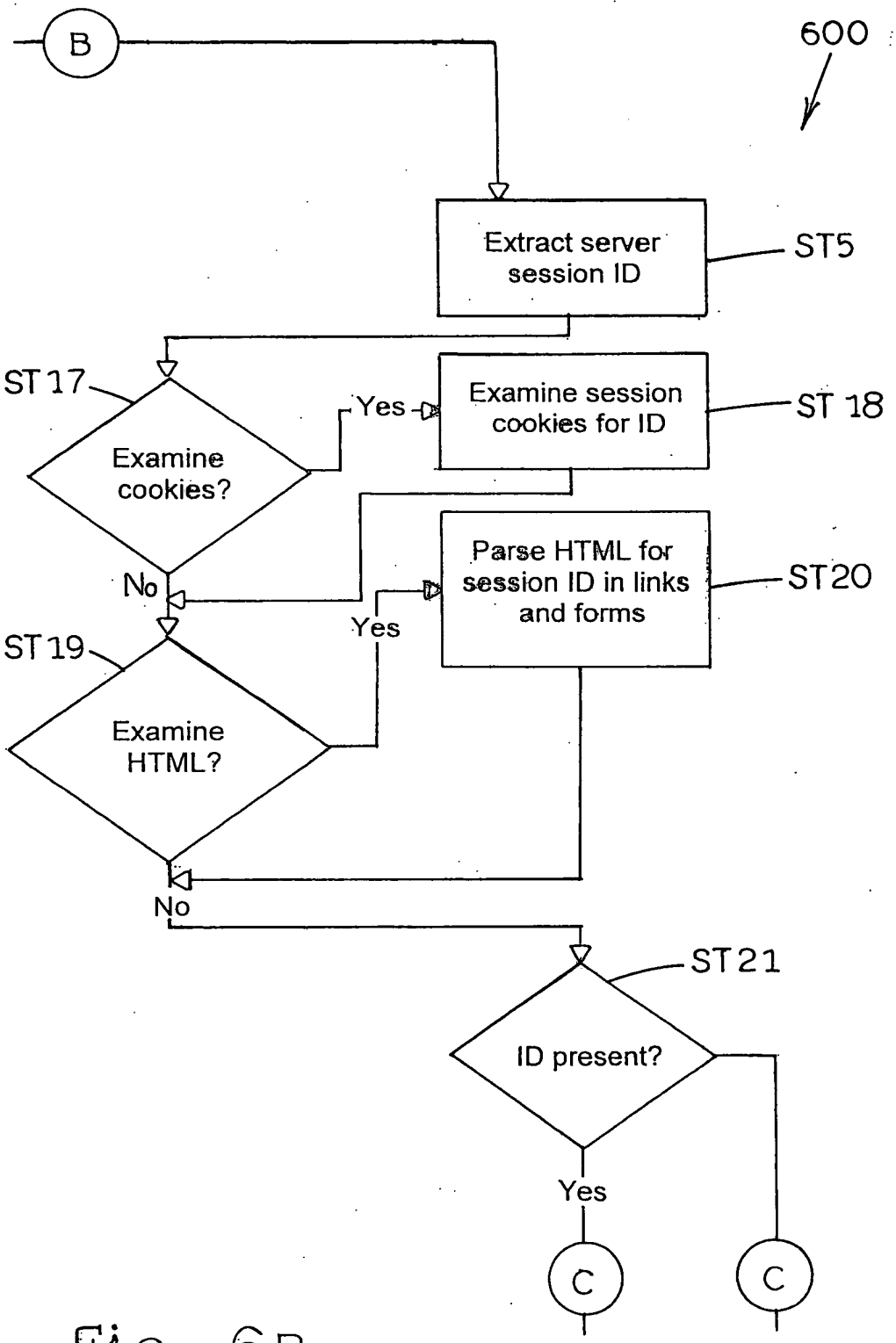
B
600
Extract server session ID
ST5
ST17
Examine cookies?
Yes
Examine session cookies for ID
ST 18
No
Parse HTML for session ID in links and forms
ST20
Yes
ST19
Examine HTML?
No
ST21
ID present?
Yes
C
C

Fig. 6B

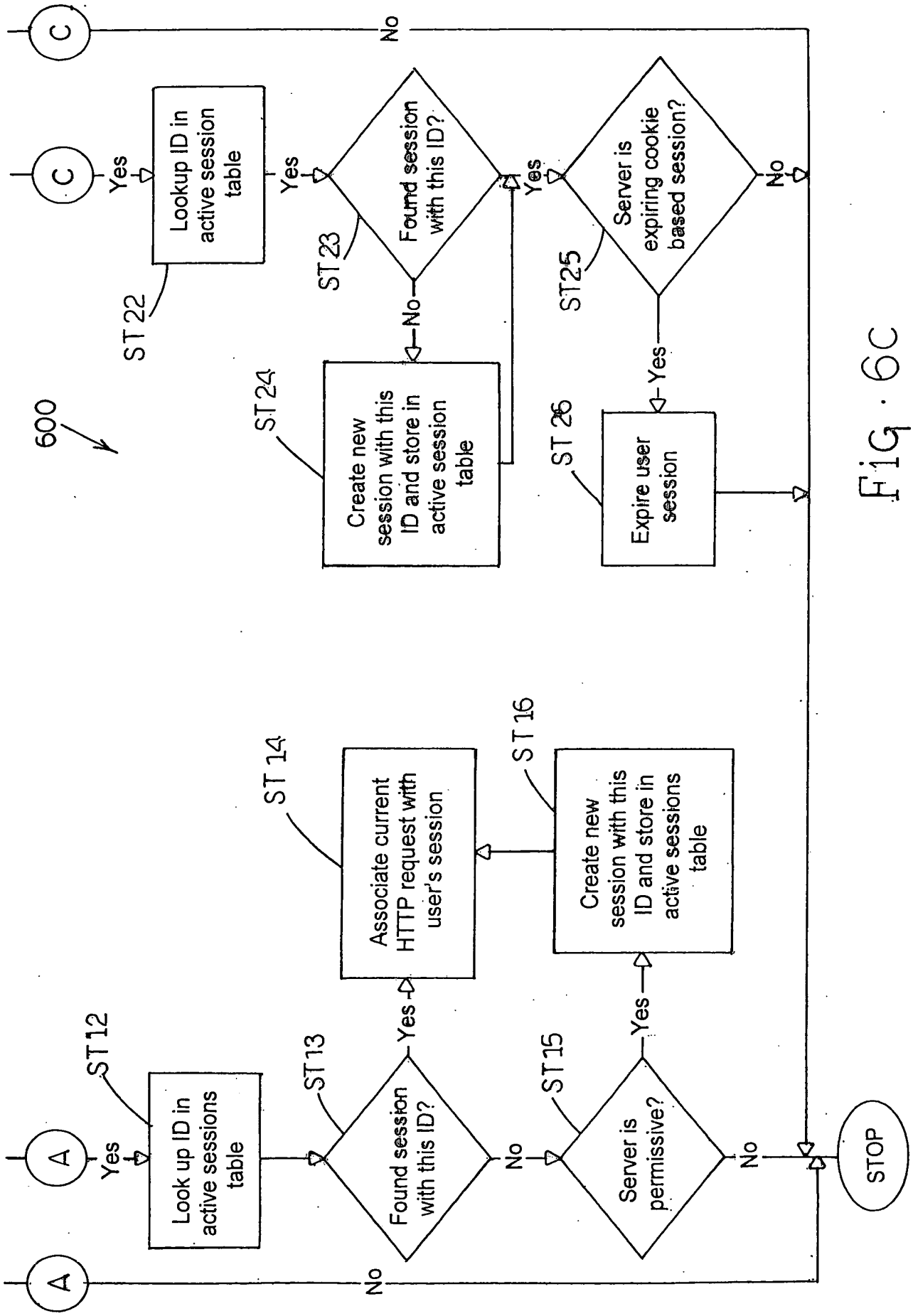
600
A
C
Yes
No
ST12
Look up ID in active sessions table
ST13
Found session with this ID?
ST14
Associate current HTTP request with user's session
ST15
Server is permissive?
ST16
Create new session with this ID and store in active sessions table
STOP
ST22
Lookup ID in active session table
ST23
Found session with this ID?
ST24
Create new session with this ID and store in active session table
ST25
Server is expiring cookie based session?
ST26
Expire user session

Fig. 6C

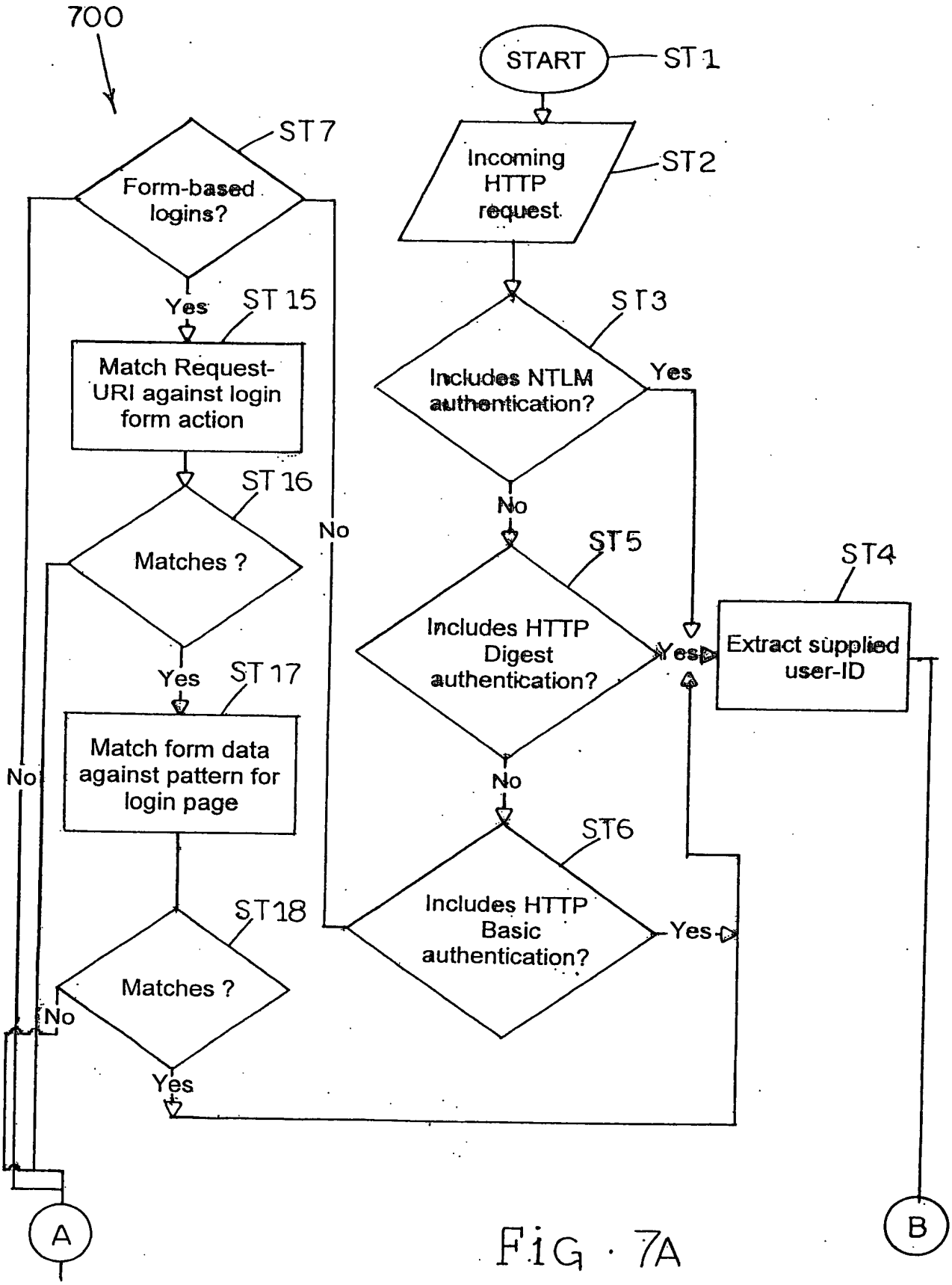
700
START
ST 1
Incoming HTTP request
ST2
ST3
Includes NTLM authentication?
Yes
No
ST5
Includes HTTP Digest authentication?
Yes
No
ST4
Extract supplied user-ID
ST6
Includes HTTP Basic authentication?
Yes
No
ST7
Form-based logins?
Yes
No
ST 15
Match Request-URI against login form action
ST 16
Matches ?
Yes
No
ST 17
Match form data against pattern for login page
ST18
Matches ?
Yes
No
A
B

FIG. 7A

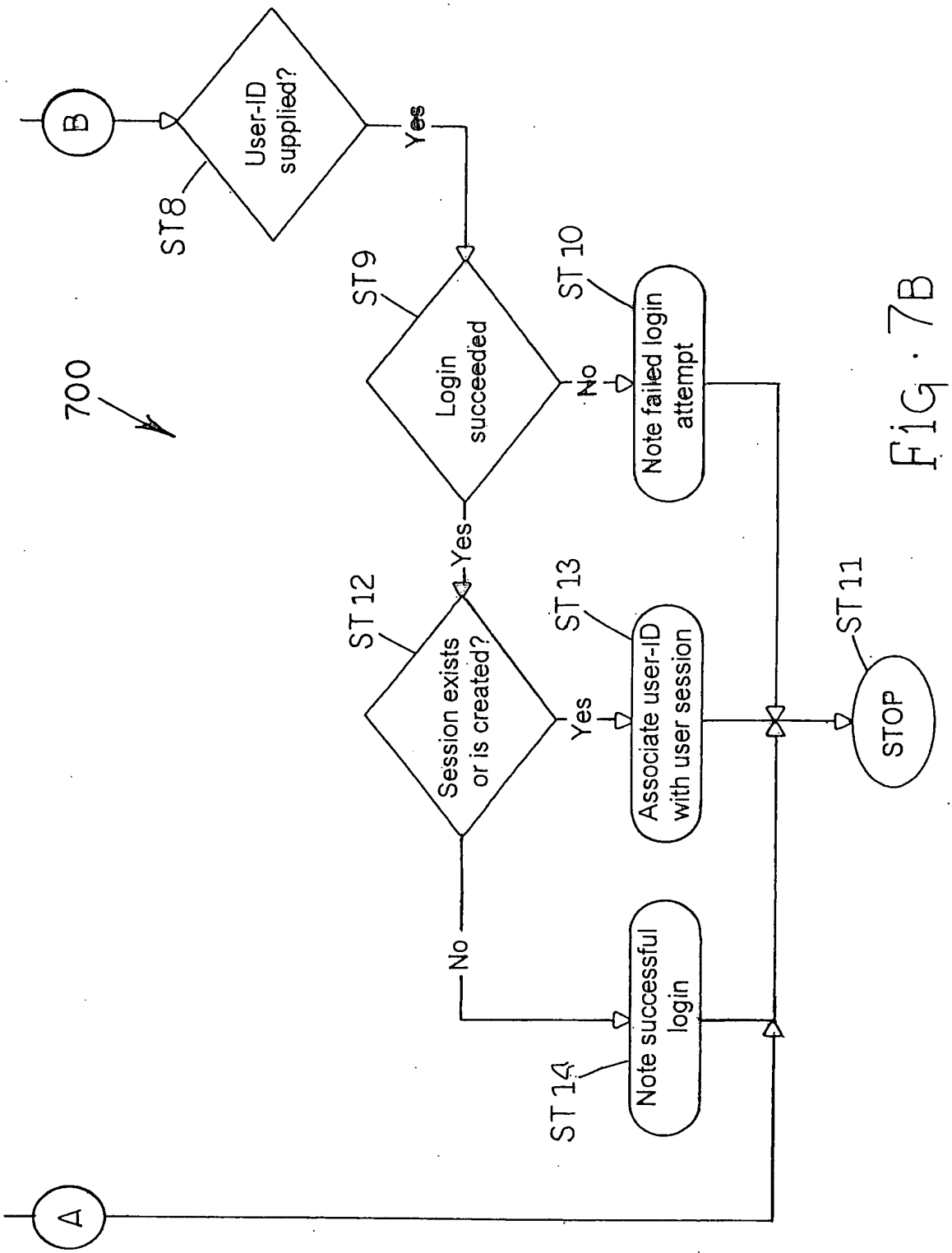
700
B
User-ID supplied?
ST8
Yes
ST9
Login succeeded
No
ST10
Note failed login attempt
Yes
ST12
Session exists or is created?
Yes
ST13
Associate user-ID with user session
ST11
STOP
No
ST14
Note successful login
A

FIG. 7B

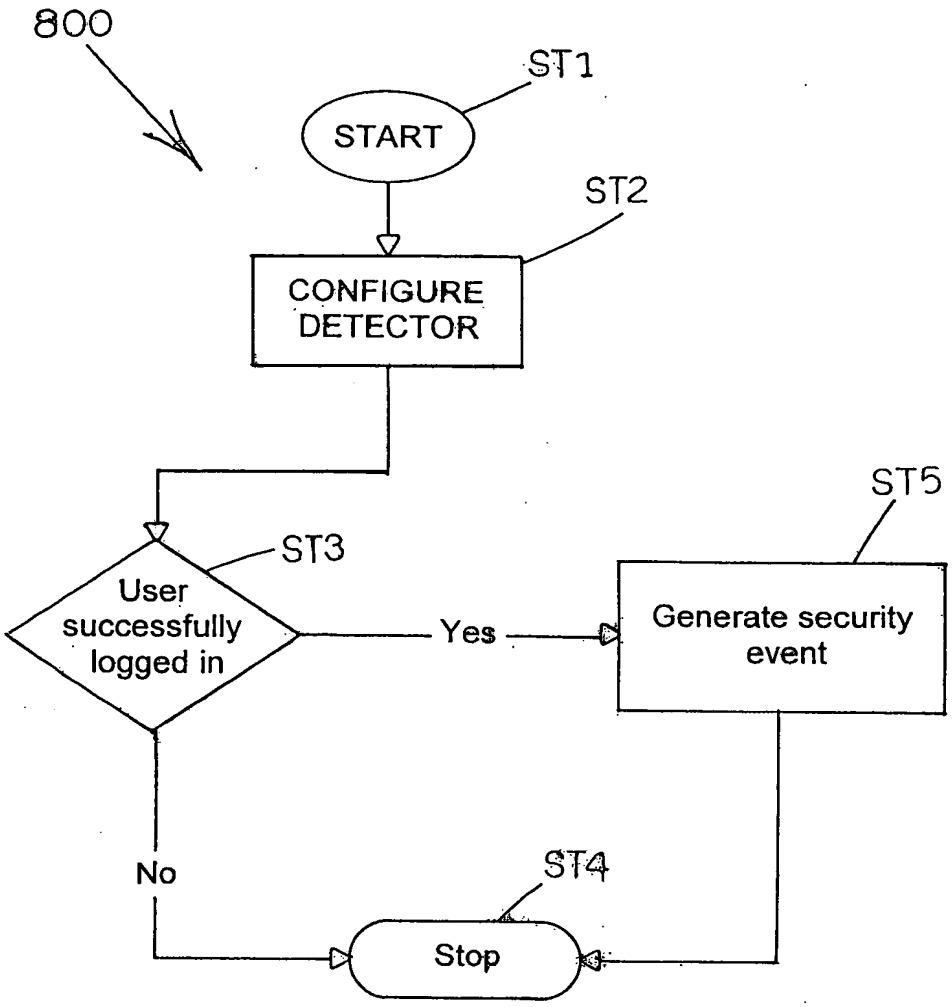
800
ST1
START
ST2
CONFIGURE DETECTOR
ST3
User successfully logged in
Yes
ST5
Generate security event
No
ST4
Stop

FIG. 8

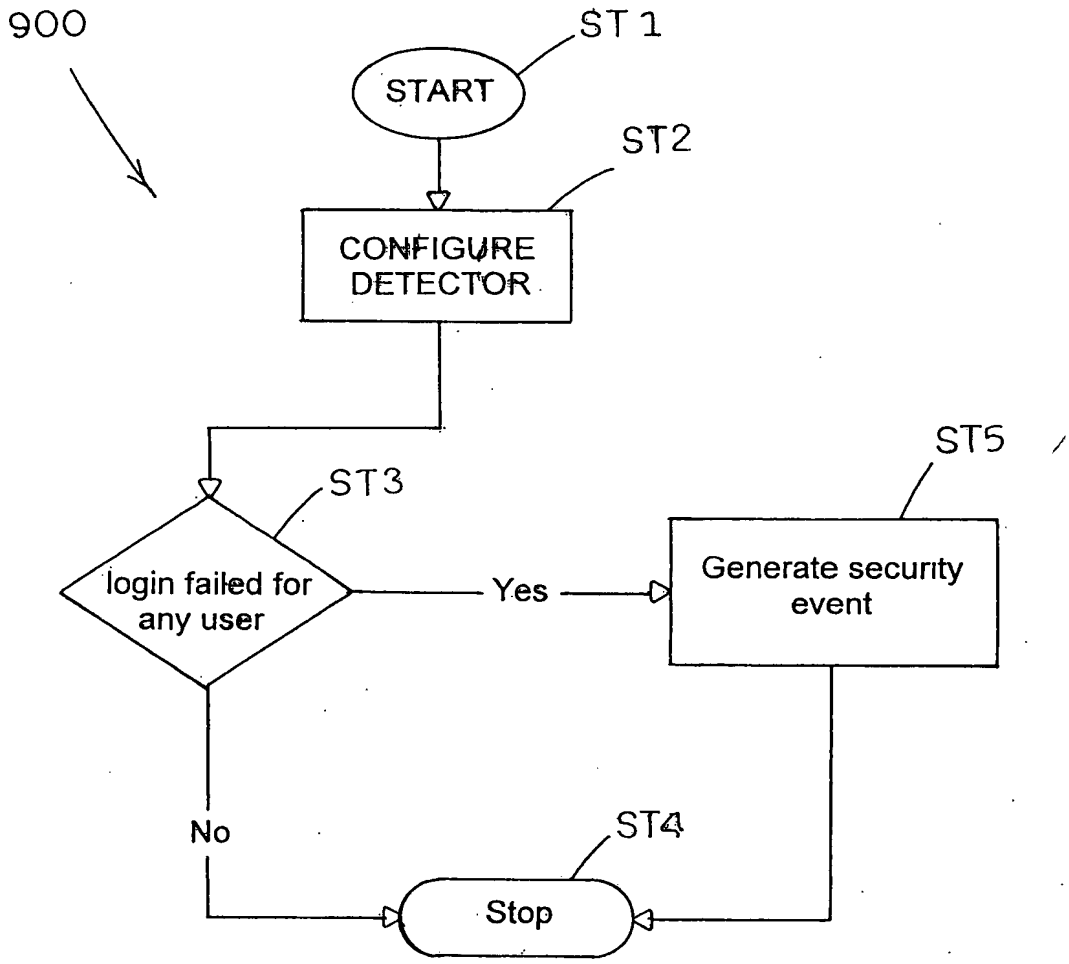
900
ST 1
START
ST2
CONFIGURE DETECTOR
ST3
login failed for any user
Yes
ST5
Generate security event
No
ST4
Stop

FIG. 9

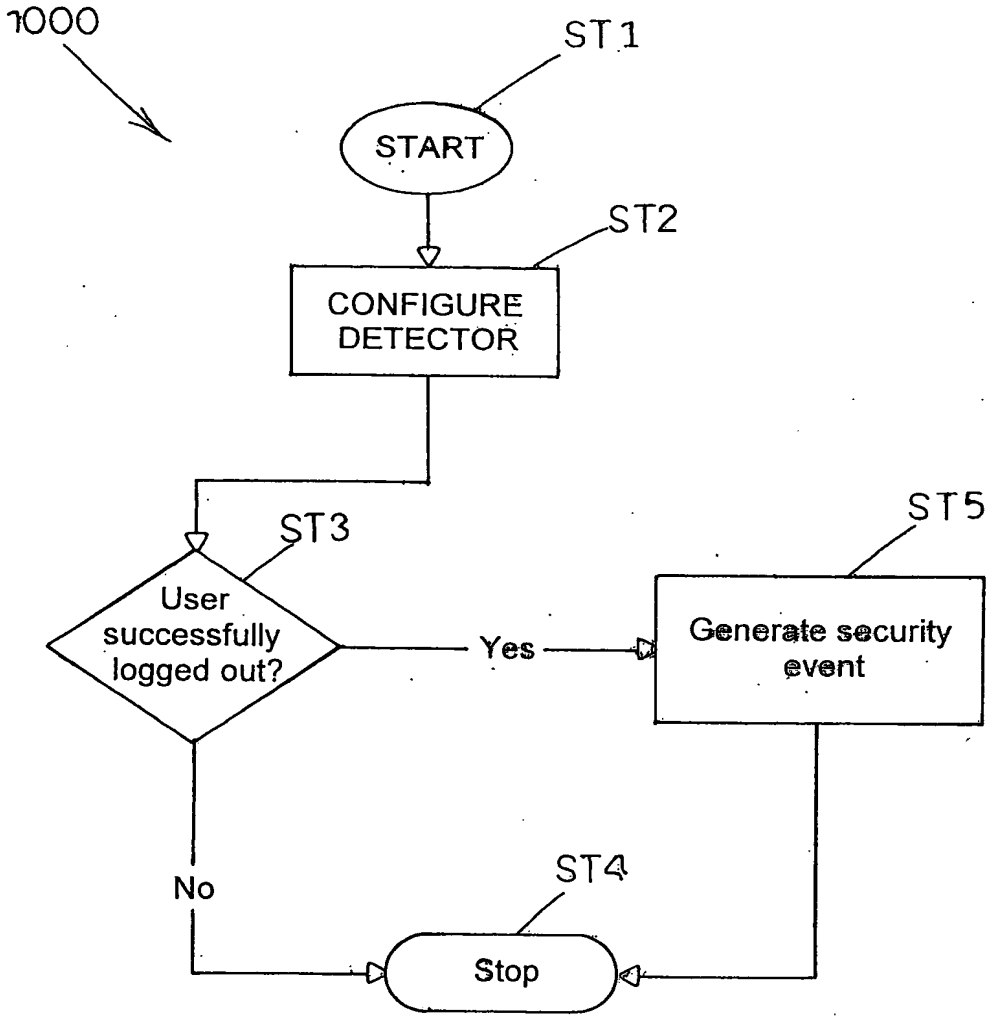
1000
ST1
START
ST2
CONFIGURE DETECTOR
ST3
User successfully logged out?
Yes
ST5
Generate security event
No
ST4
Stop

Fig. 10

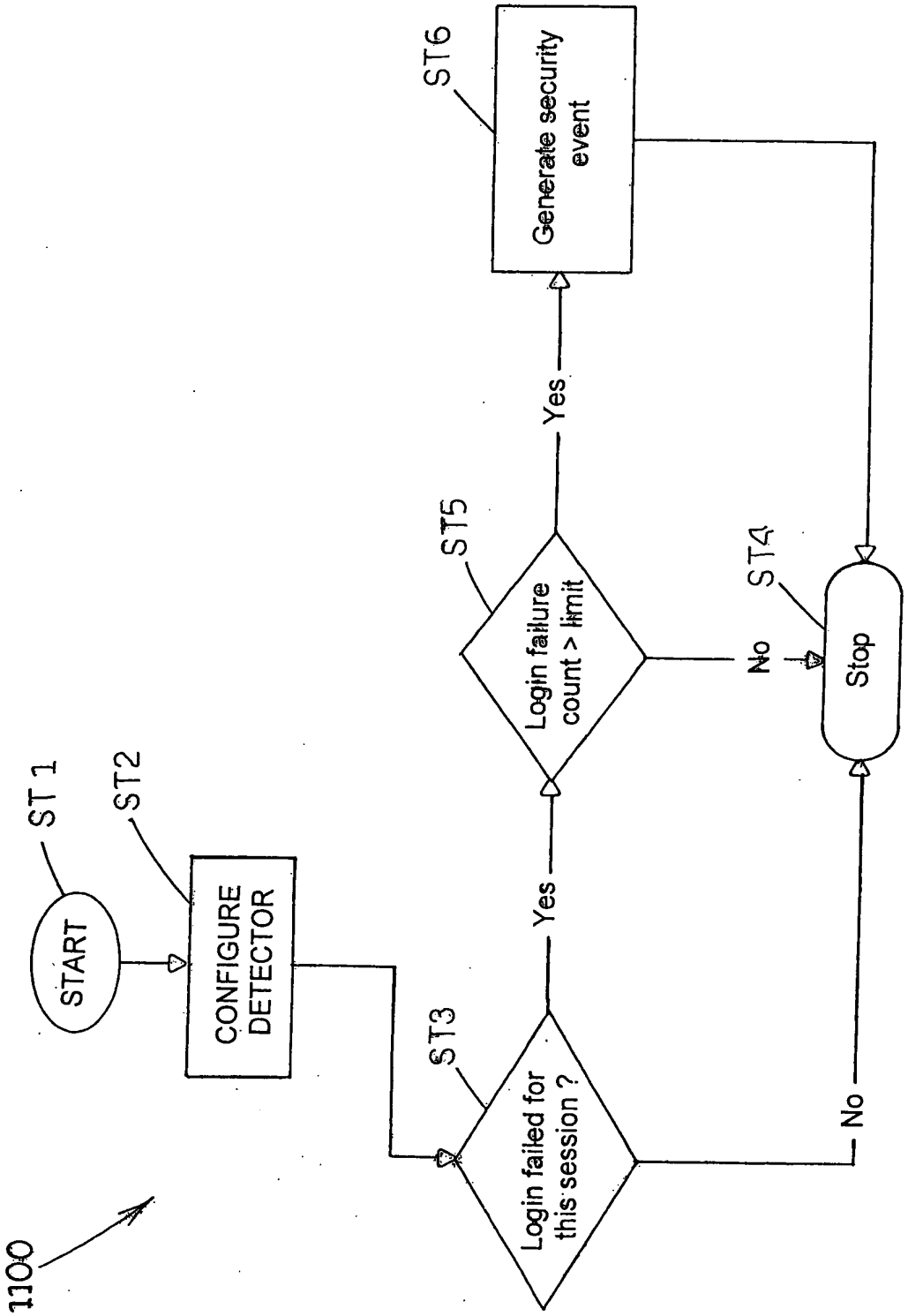
1100
START
ST 1
CONFIGURE DETECTOR
ST2
Login failed for this session ?
ST3
Yes
No
Login failure count > limit
ST5
Yes
No
Stop
ST4
Generate security event
ST6

FIG. 11

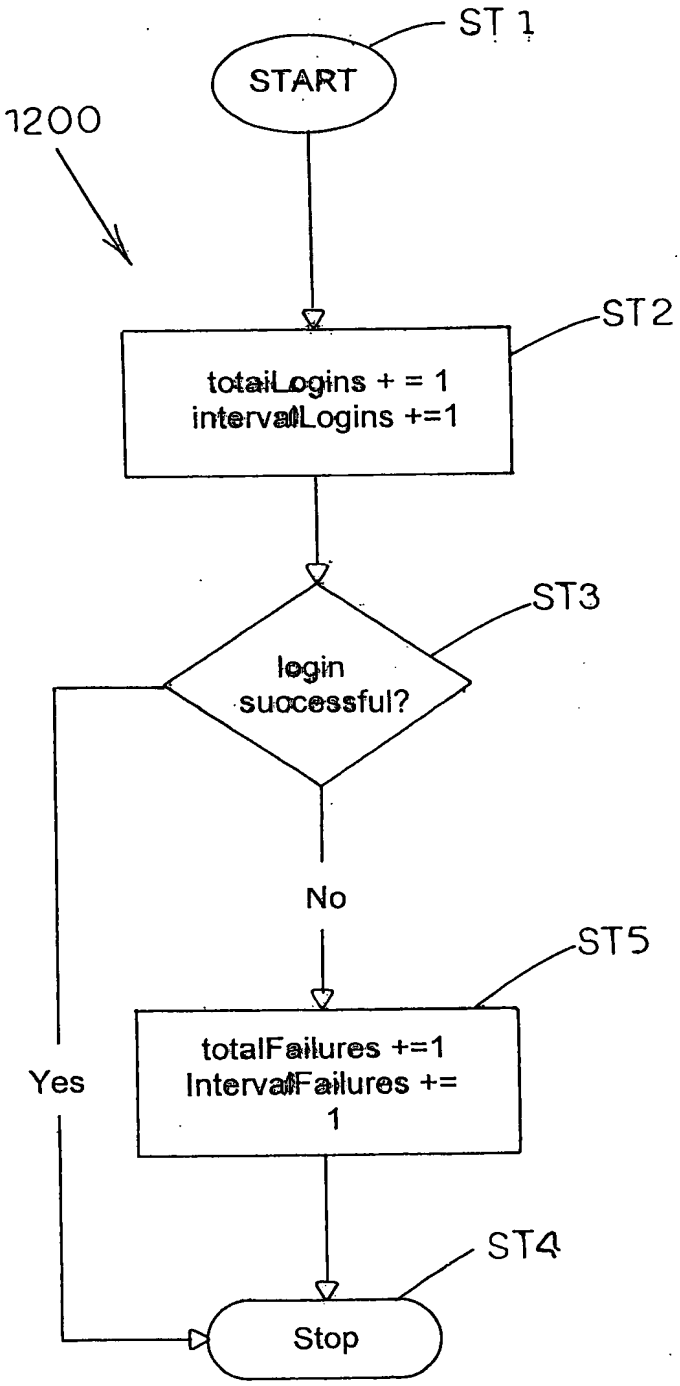
ST 1
START
1200
ST2
totalLogins + = 1
intervalLogins +=1
ST3
login successful?
No
ST5
totalFailures +=1
IntervalFailures += 1
Yes
ST4
Stop

Fig. 12A

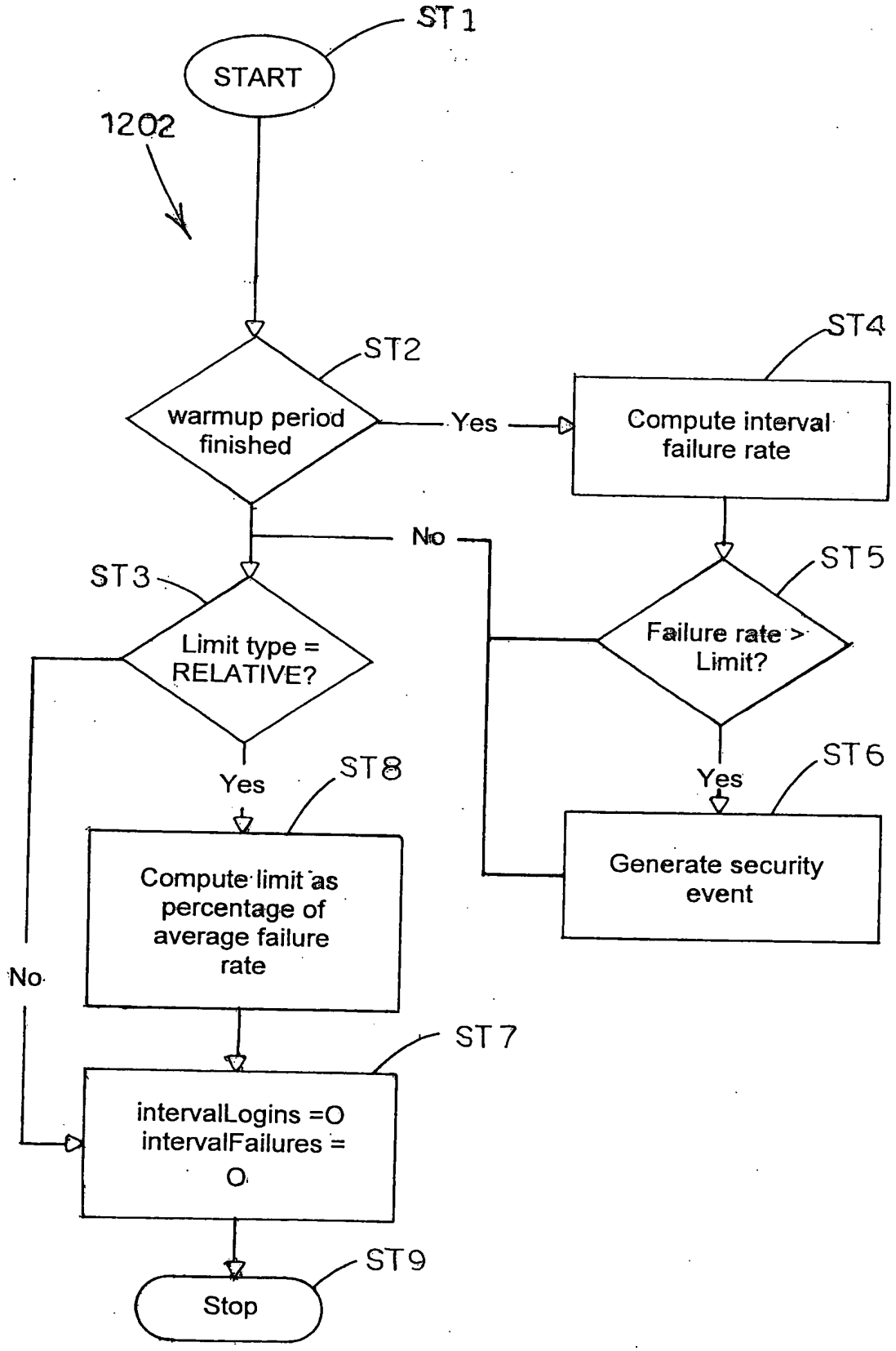
ST 1
START
1202
ST2
warmup period finished
Yes
ST4
Compute interval failure rate
No
ST3
Limit type = RELATIVE?
ST5
Failure rate > Limit?
Yes
ST8
Yes
ST6
Compute limit as percentage of average failure rate
Generate security event
No
ST 7
intervalLogins =O
intervalFailures = O
ST9
Stop

FIG. 12B

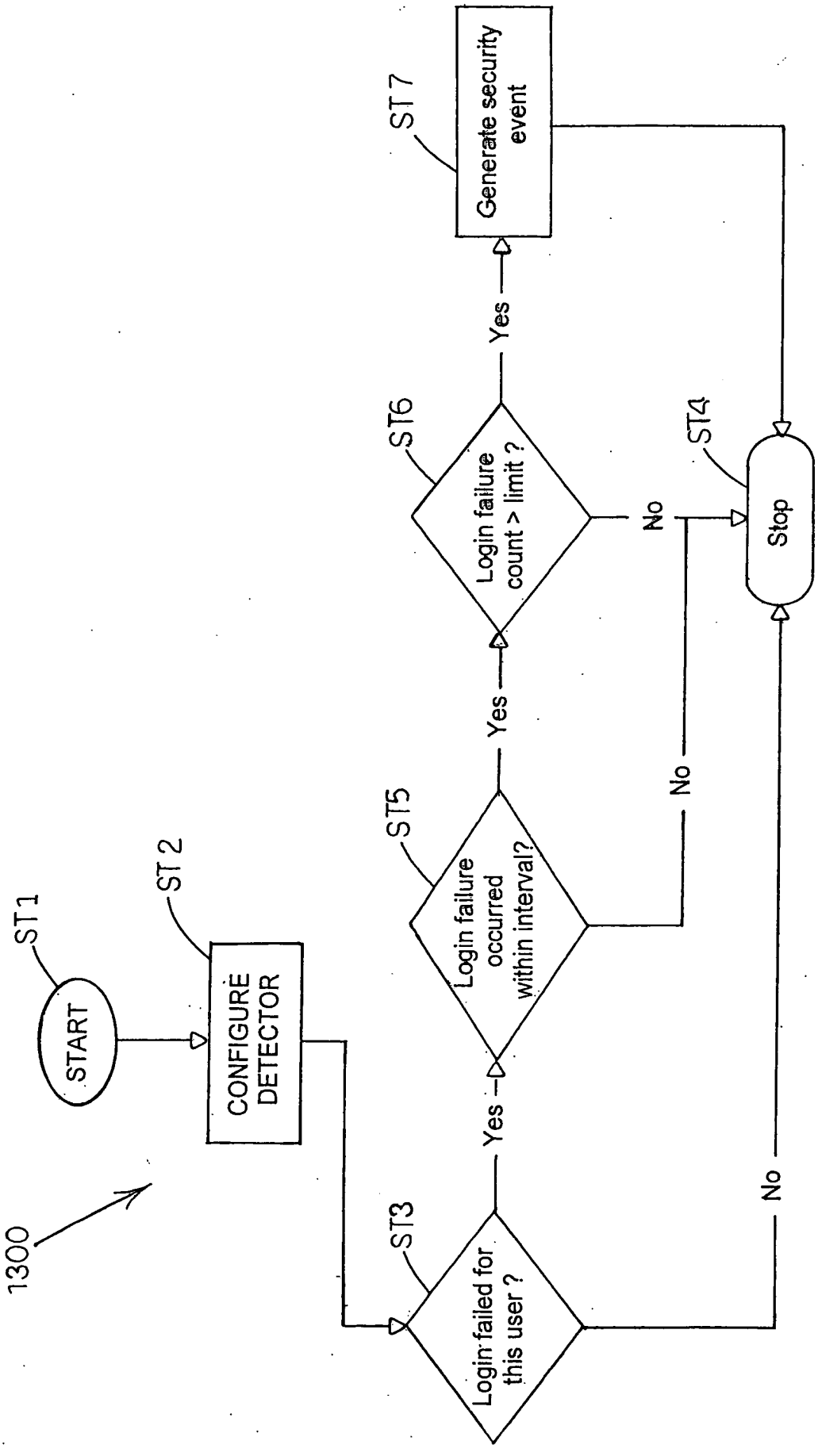
1300
ST1
START
ST 2
CONFIGURE DETECTOR
ST3
Login failed for this user ?
Yes
No
ST5
Login failure occurred within interval?
Yes
No
ST6
Login failure count > limit ?
Yes
No
ST 7
Generate security event
ST4
Stop

Fig. 13

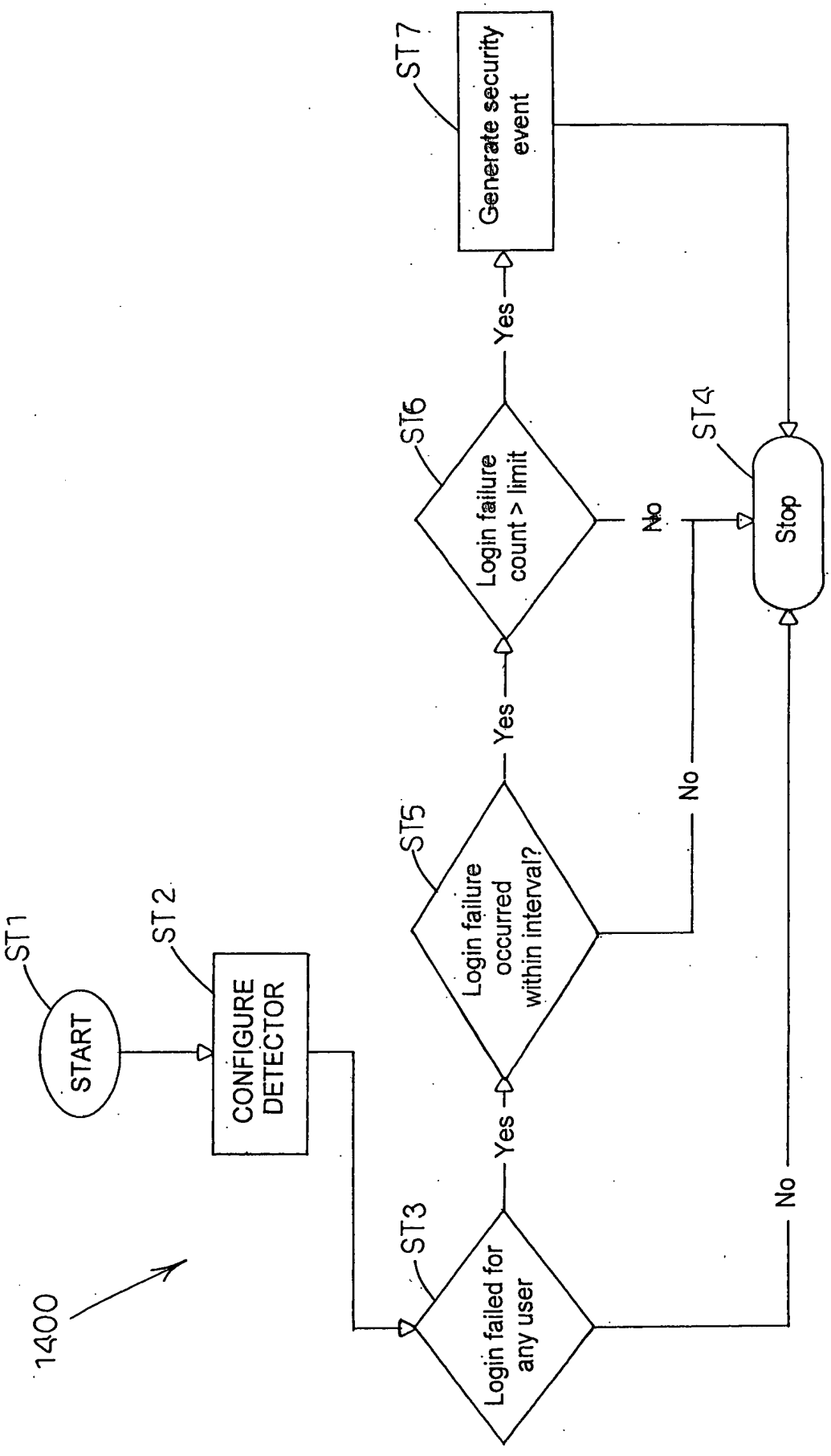
1400
ST1
START
ST2
CONFIGURE DETECTOR
ST3
Login failed for any user
Yes
ST5
Login failure occurred within interval?
Yes
ST6
Login failure count > limit
Yes
ST7
Generate security event
No
No
No
ST4
Stop

FIG. 14

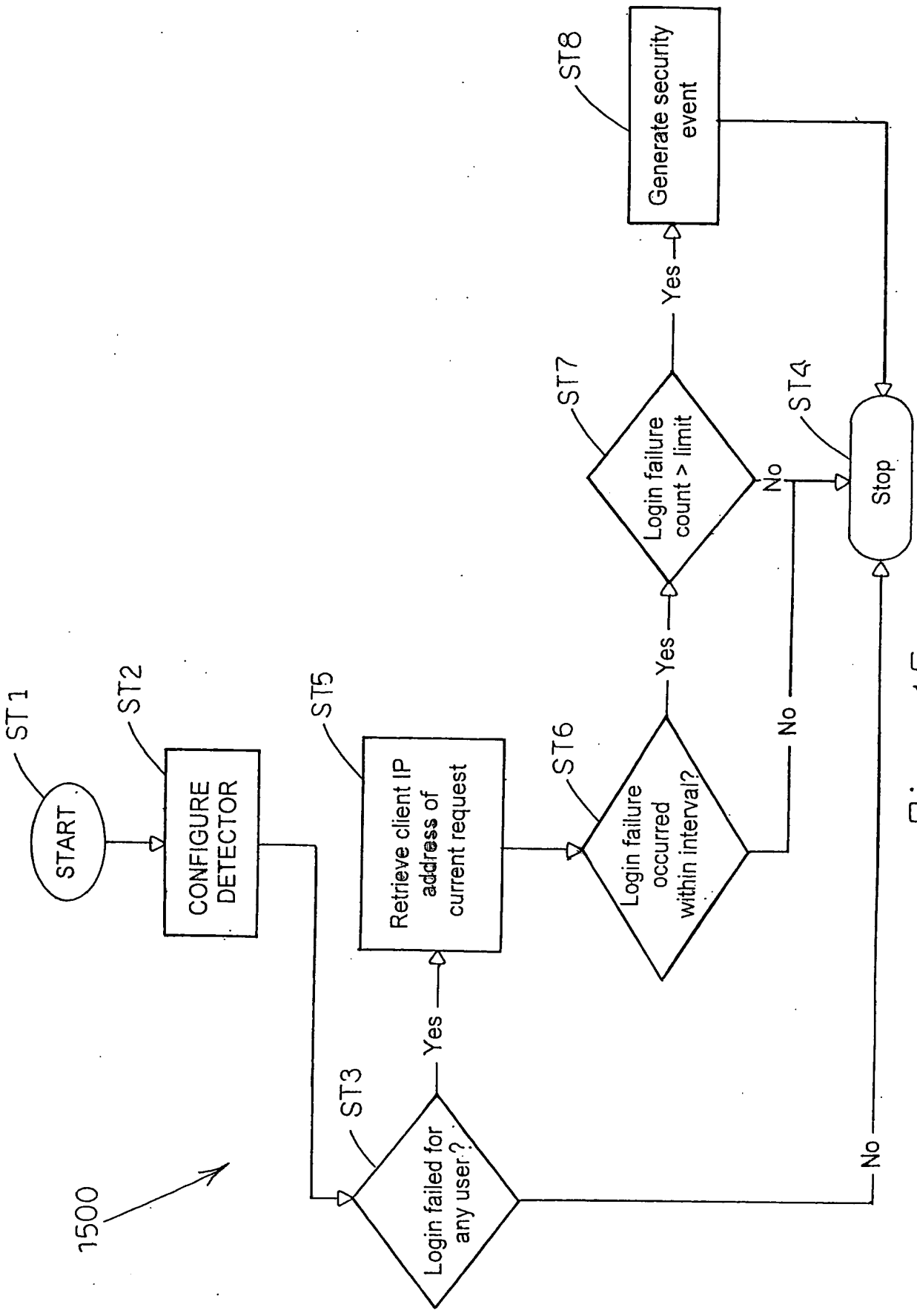
1500
START
ST1
CONFIGURE DETECTOR
ST2
Login failed for any user?
ST3
Yes
No
Retrieve client IP address of current request
ST5
Login failure occurred within interval?
ST6
Yes
No
Login failure count > limit
ST7
Yes
No
Generate security event
ST8
Stop
ST4

Fig. 15A

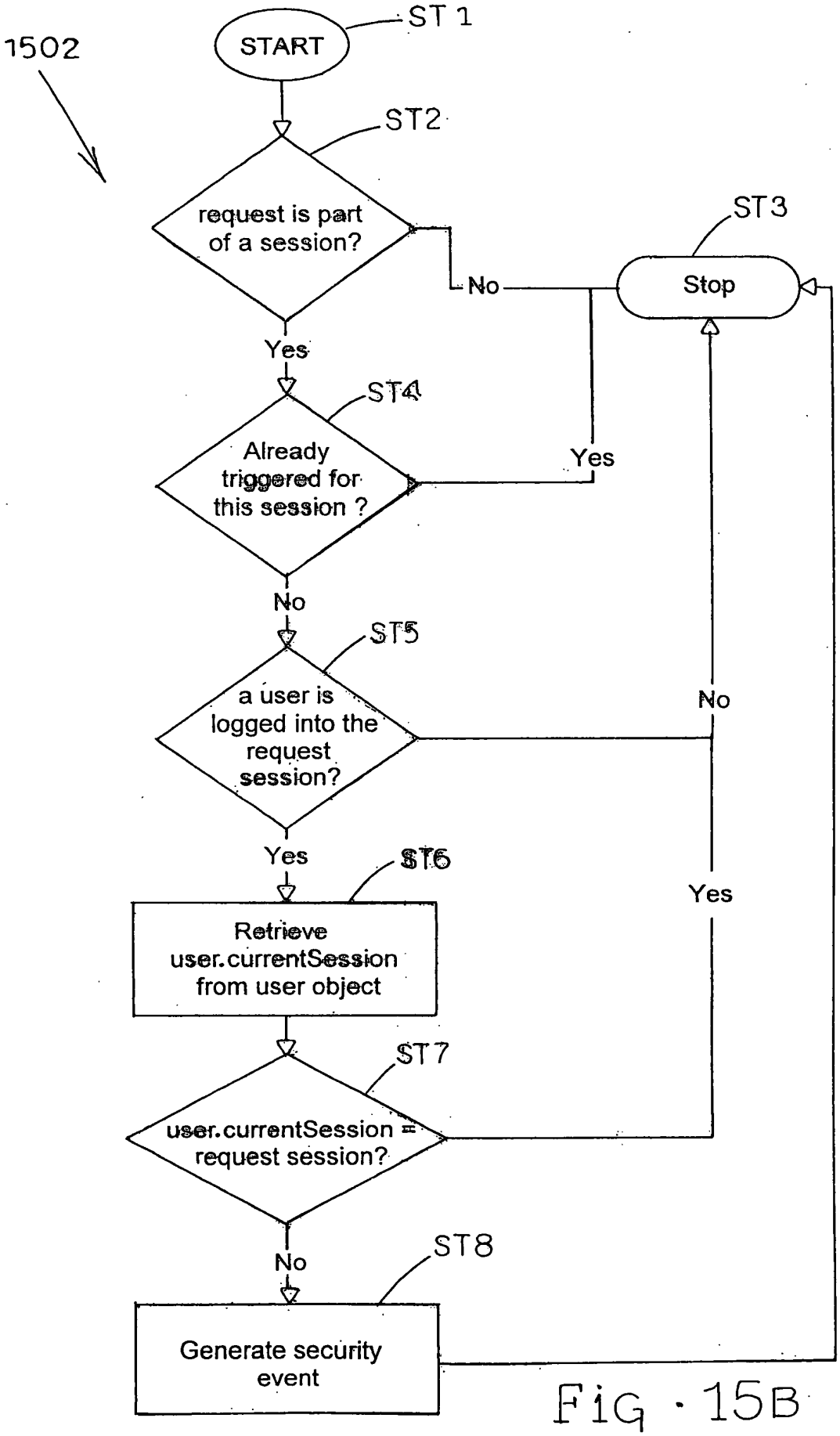
1502
START
ST 1
ST2
request is part of a session?
No
ST3
Stop
Yes
ST4
Already triggered for this session ?
Yes
No
ST5
a user is logged into the request session?
No
Yes
ST6
Retrieve user.currentSession from user object
ST7
user.currentSession = request session?
Yes
No
ST8
Generate security event

Fig · 15B

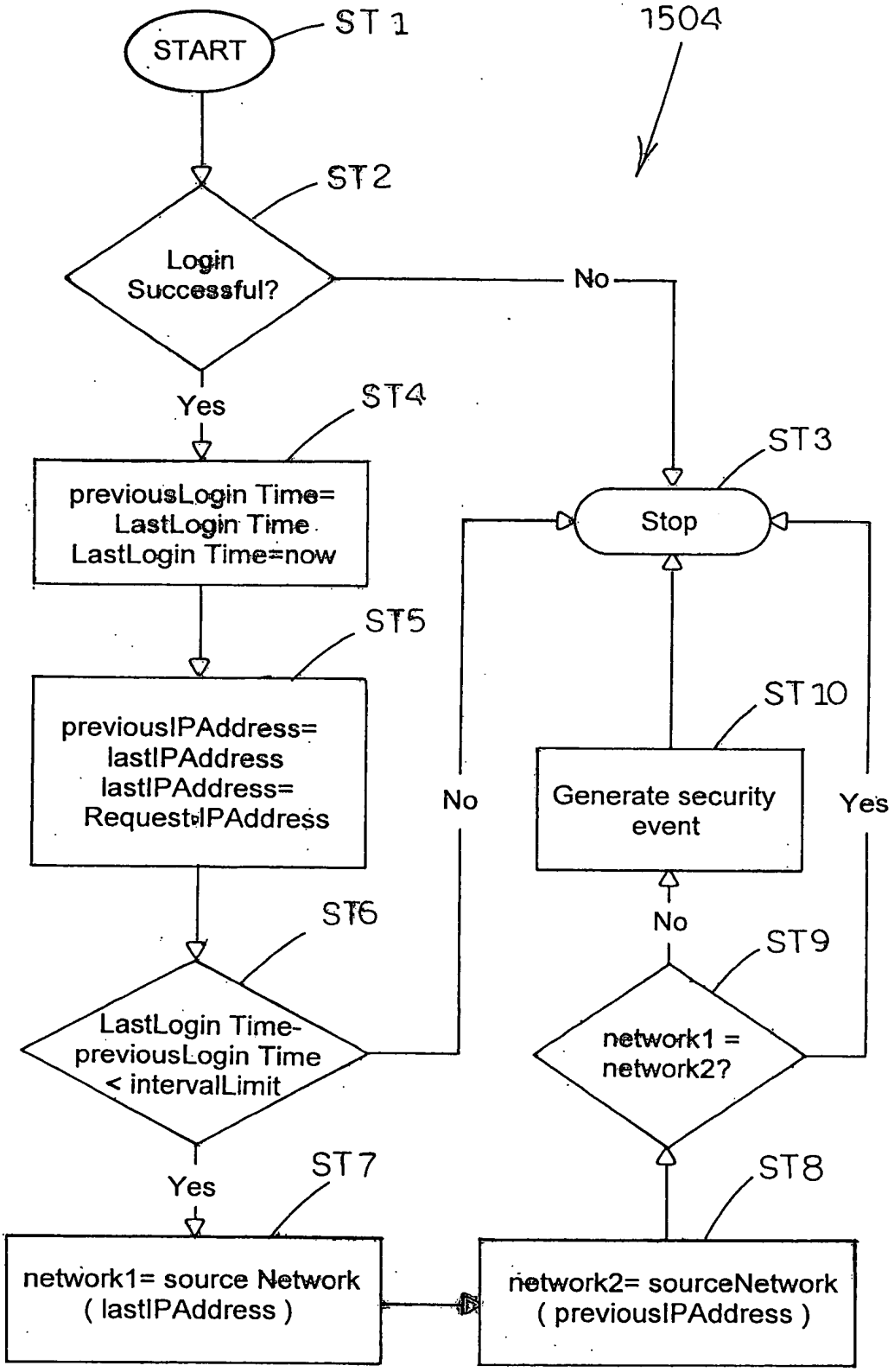
START
ST 1
1504
ST2
Login Successful?
No
Yes
ST4
previousLogin Time= LastLogin Time
LastLogin Time=now
ST3
Stop
ST5
previousIPAddress= lastIPAddress
lastIPAddress= RequestIPAddress
ST 10
Generate security event
No
Yes
ST6
LastLogin Time- previousLogin Time < intervalLimit
No
ST9
network1 = network2?
Yes
ST7
ST8
network1= source Network (lastIPAddress)
network2= sourceNetwork (previousIPAddress)

Fig. 15c

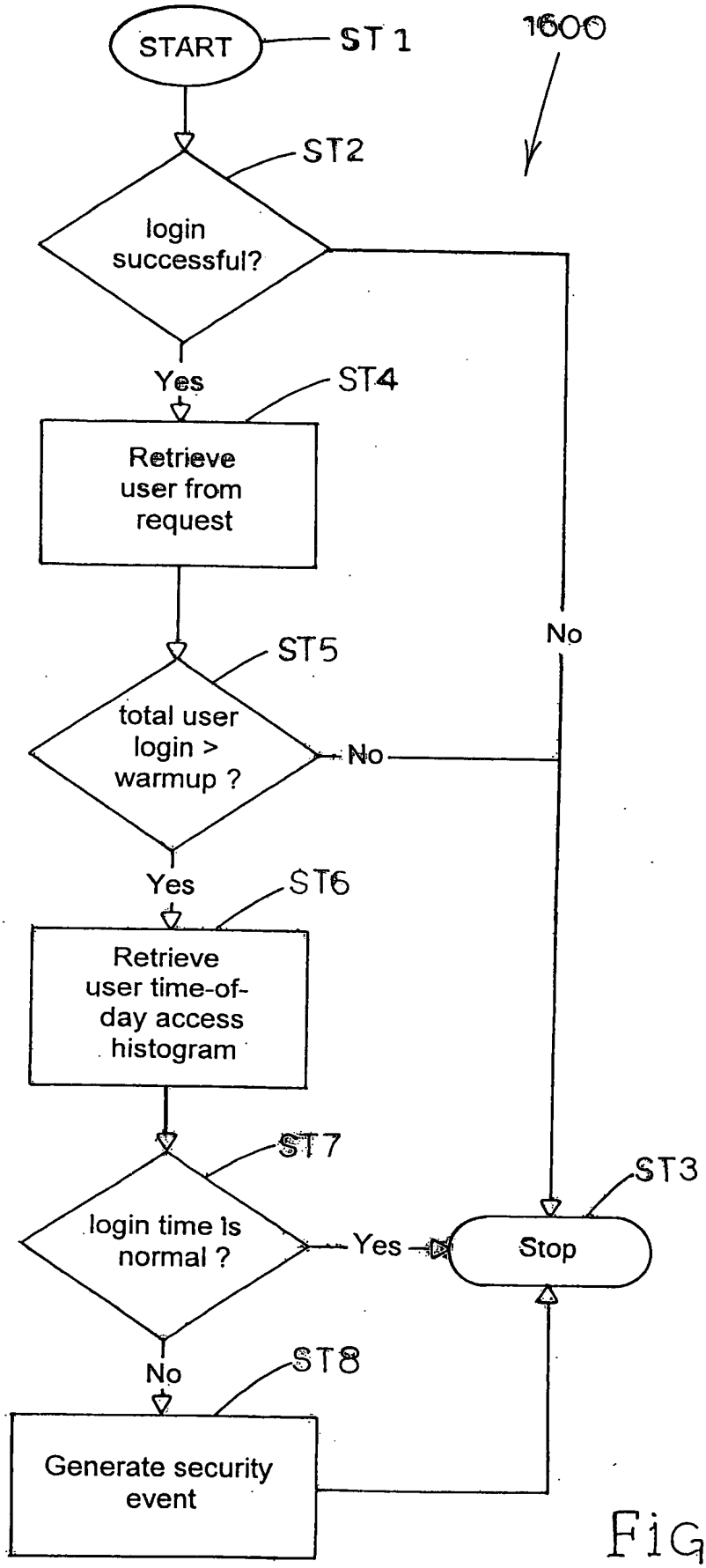
START
ST 1
1600
ST2
login successful?
Yes
ST4
Retrieve user from request
No
ST5
total user login > warmup ?
No
Yes
ST6
Retrieve user time-of-day access histogram
ST7
login time is normal ?
Yes
ST3
Stop
No
ST8
Generate security event

Fig. 16A

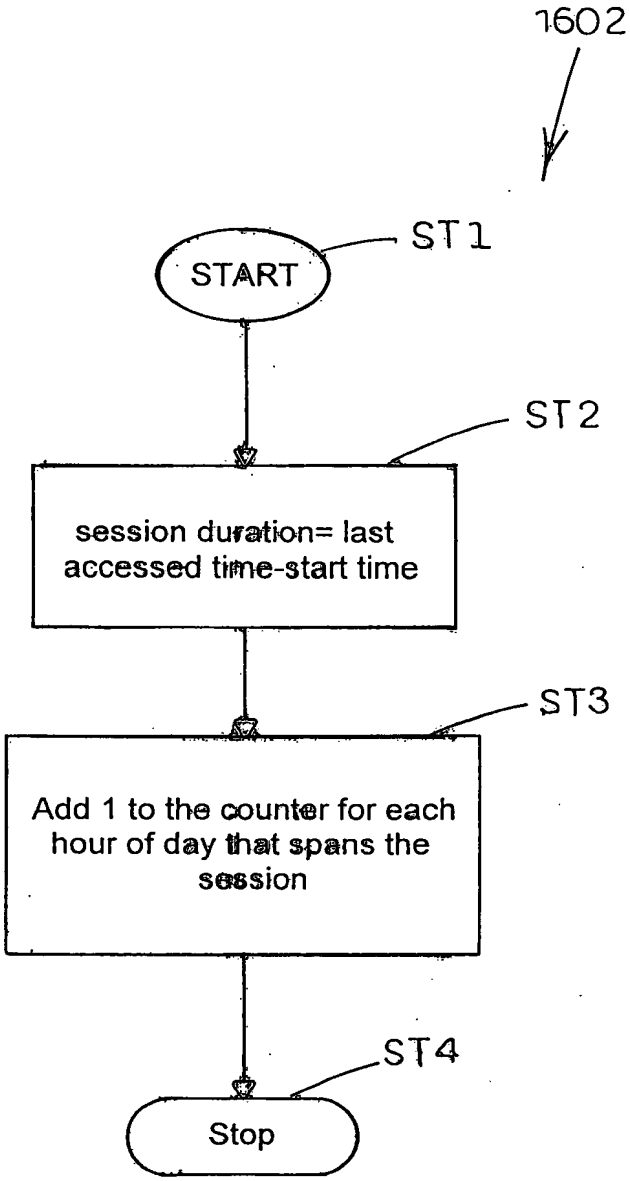
1602
START
ST1
ST2
session duration= last accessed time-start time
ST3
Add 1 to the counter for each hour of day that spans the session
ST4
Stop

Fig. 16B

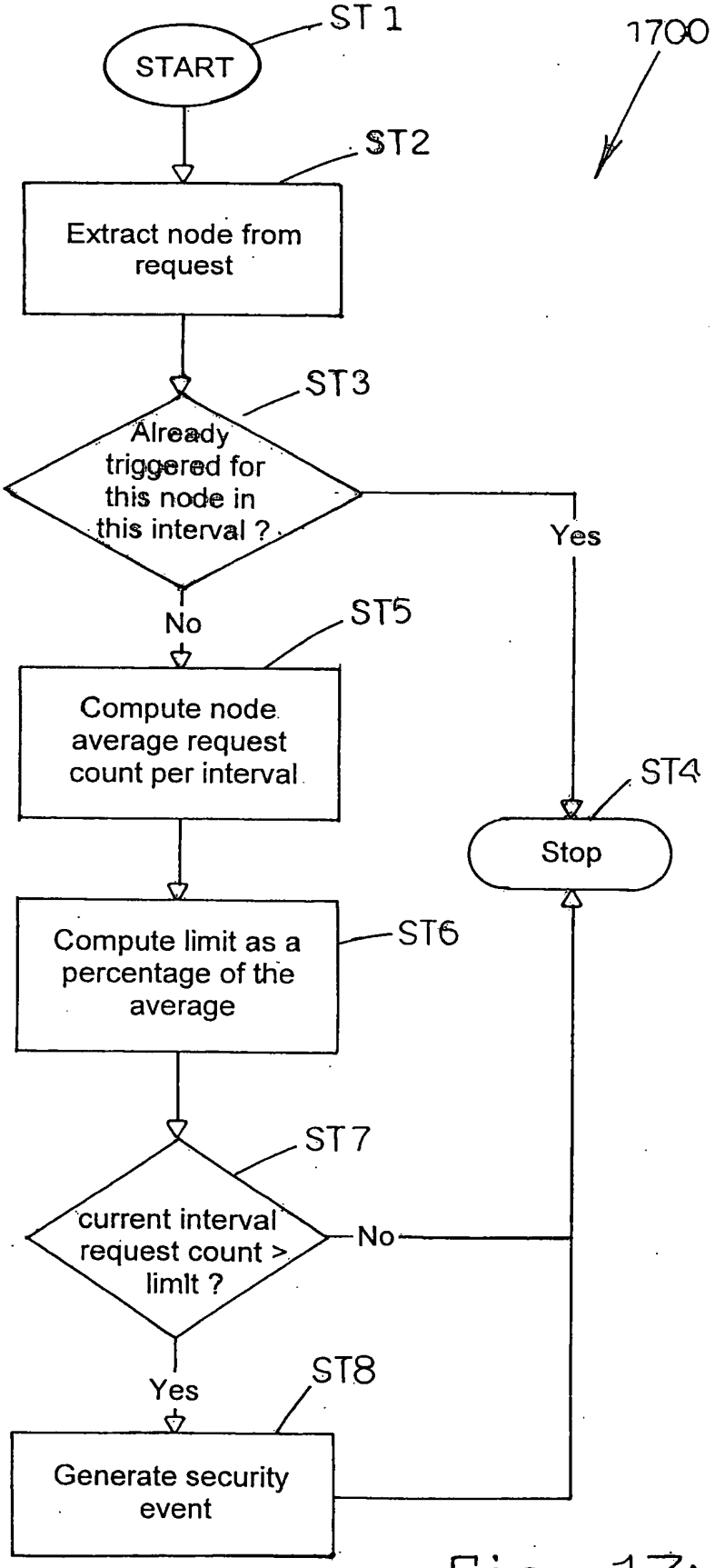
1700
ST 1
START
ST2
Extract node from request
ST3
Already triggered for this node in this interval ?
Yes
No
ST5
Compute node average request count per interval
ST4
Stop
Compute limit as a percentage of the average
ST6
ST 7
current interval request count > limIt ?
No
Yes
ST8
Generate security event

Fig. 17A

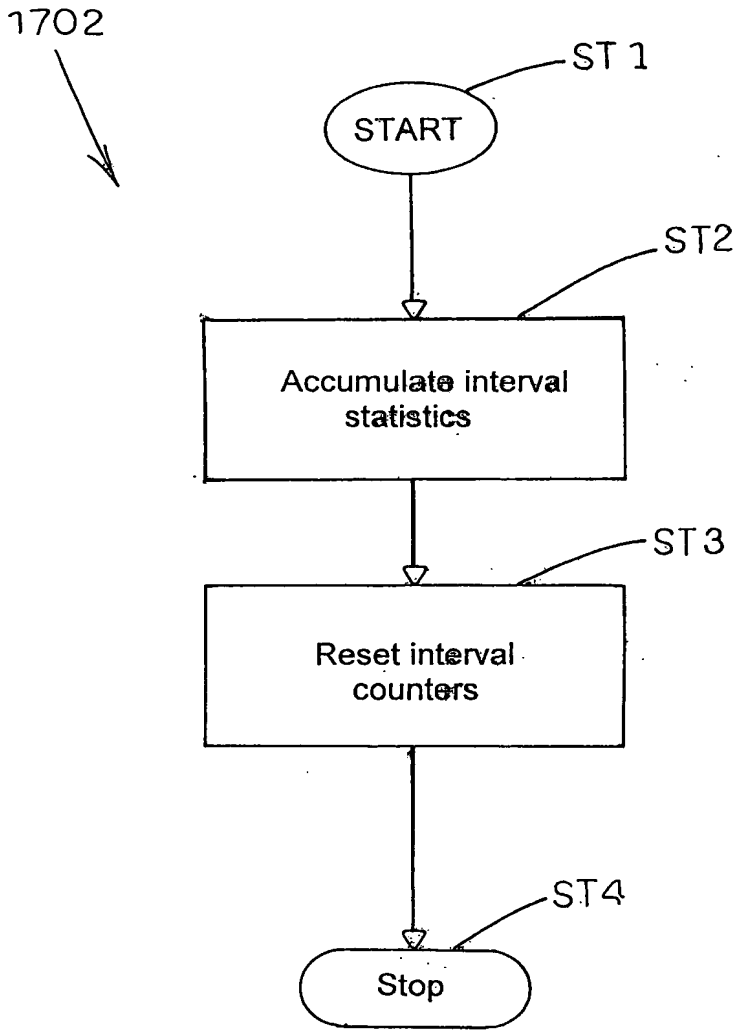
1702
ST 1
START
ST2
Accumulate interval statistics
ST3
Reset interval counters
ST4
Stop

FIG. 17B

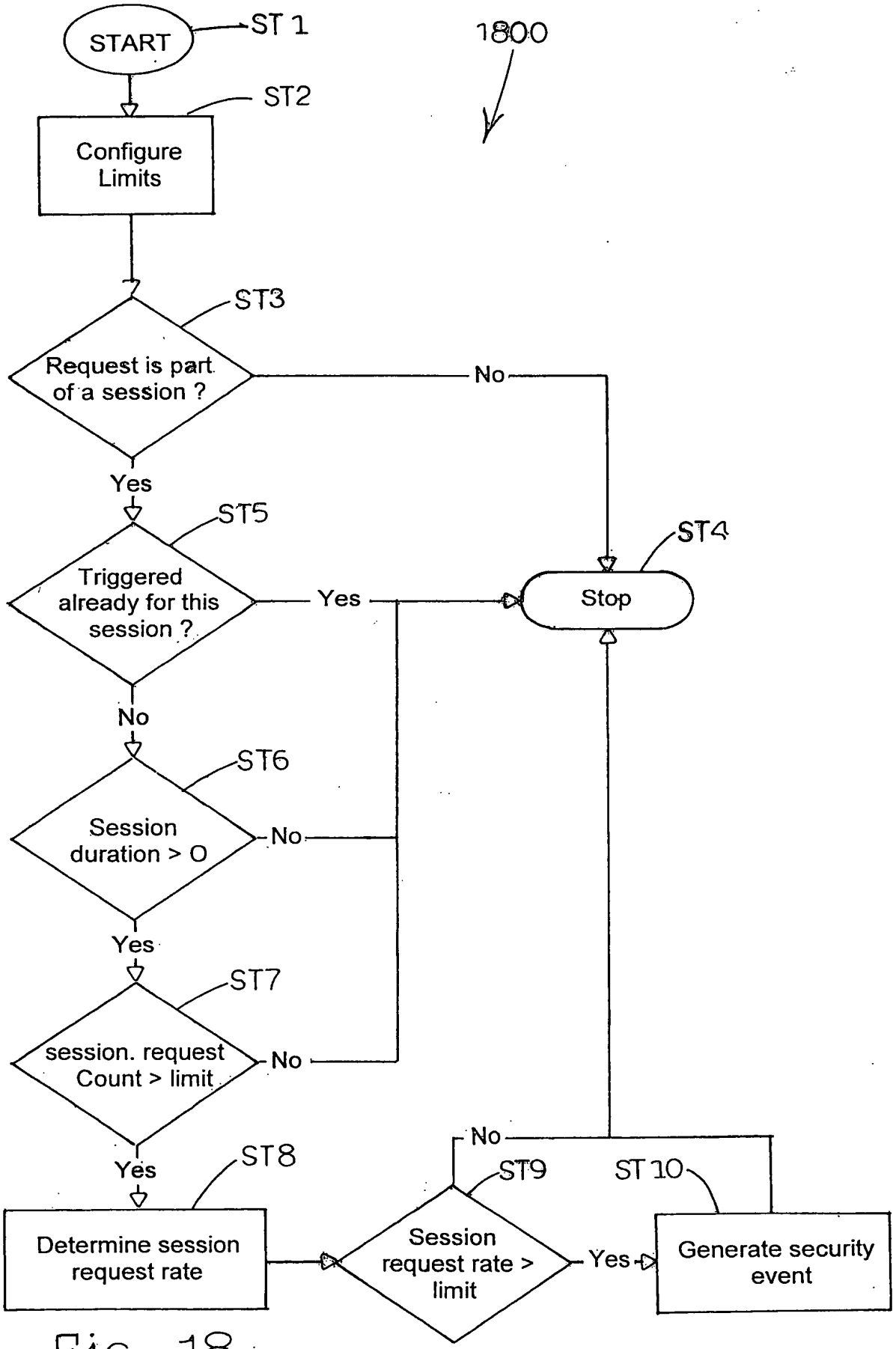
START
ST 1
1800
ST2
Configure Limits
ST3
Request is part of a session ?
No
Yes
ST5
Triggered already for this session ?
Yes
ST4
Stop
No
ST6
Session duration > 0
No
Yes
ST7
session. request Count > limit
No
Yes
ST8
Determine session request rate
ST9
Session request rate > limit
No
Yes
ST 10
Generate security event

Fig. 18

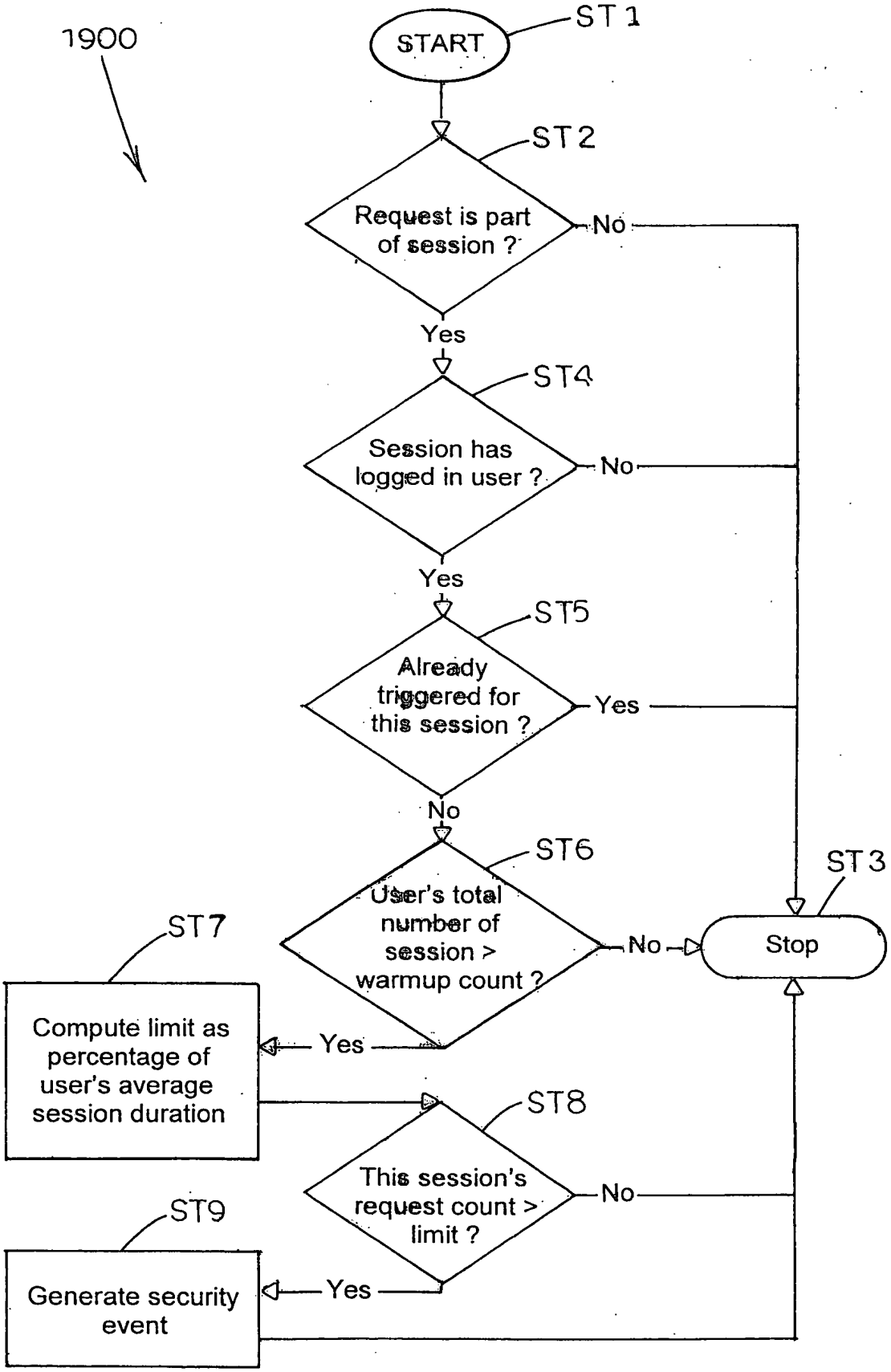
1900
START
ST 1
ST 2
Request is part of session ?
No
Yes
ST4
Session has logged in user ?
No
Yes
ST5
Already triggered for this session ?
Yes
No
ST6
User's total number of session > warmup count ?
No
ST 3
Stop
ST7
Compute limit as percentage of user's average session duration
Yes
ST8
This session's request count > limit ?
No
ST9
Generate security event
Yes

FIG · 19A

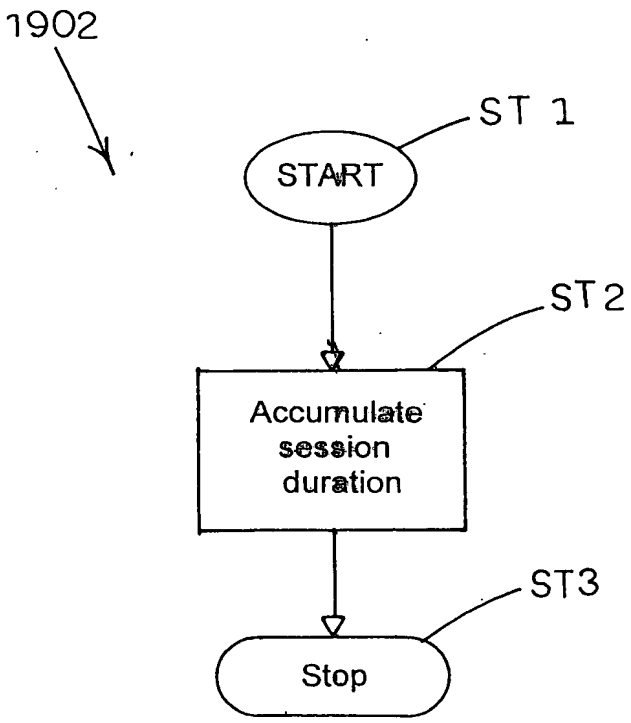

Fig. 19B

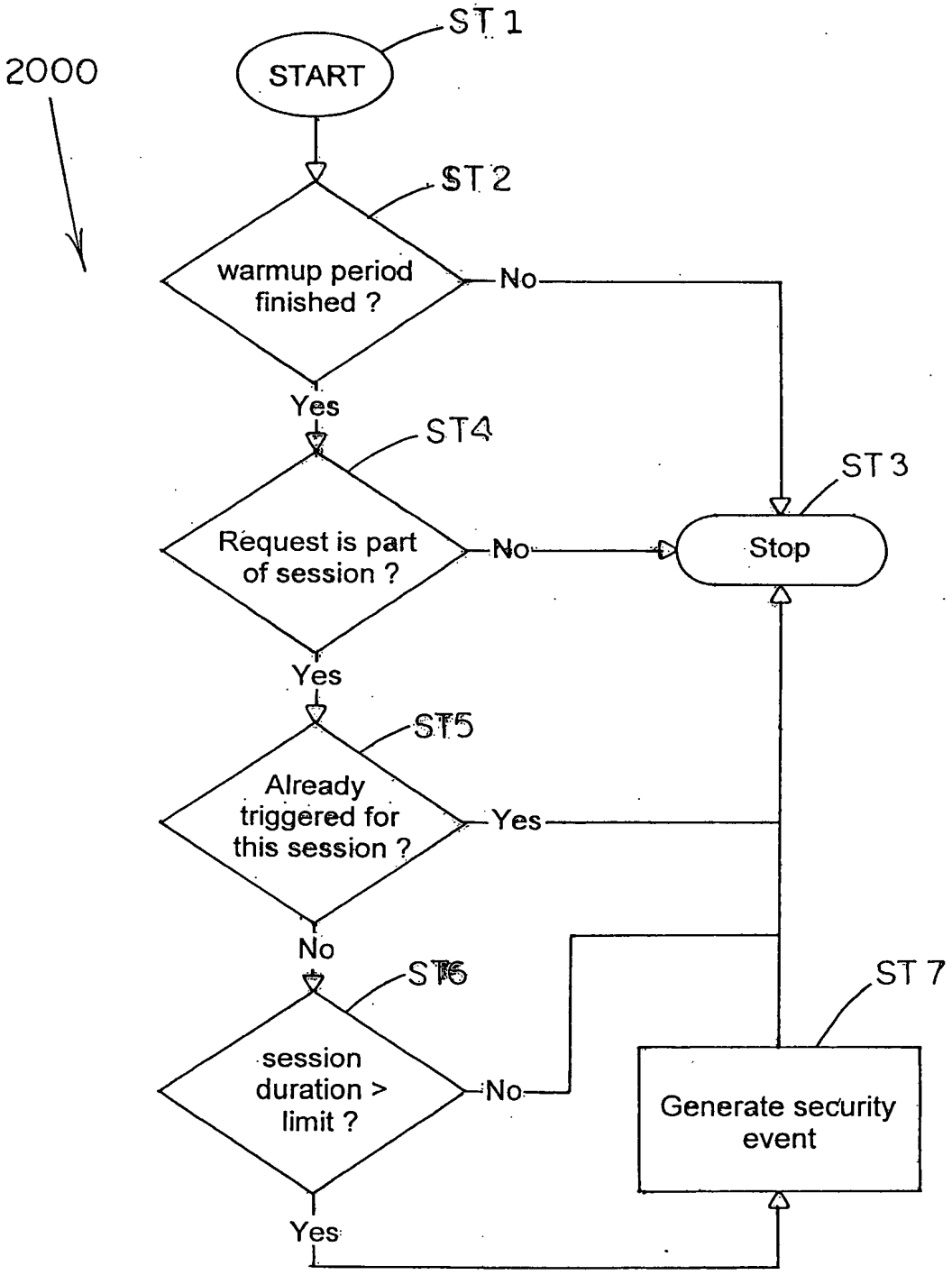
2000
START
ST 1
ST 2
warmup period finished ?
No
Yes
ST4
Request is part of session ?
No
ST 3
Stop
Yes
ST5
Already triggered for this session ?
Yes
No
ST6
session duration > limit ?
No
ST 7
Generate security event
Yes

FIG · 20A

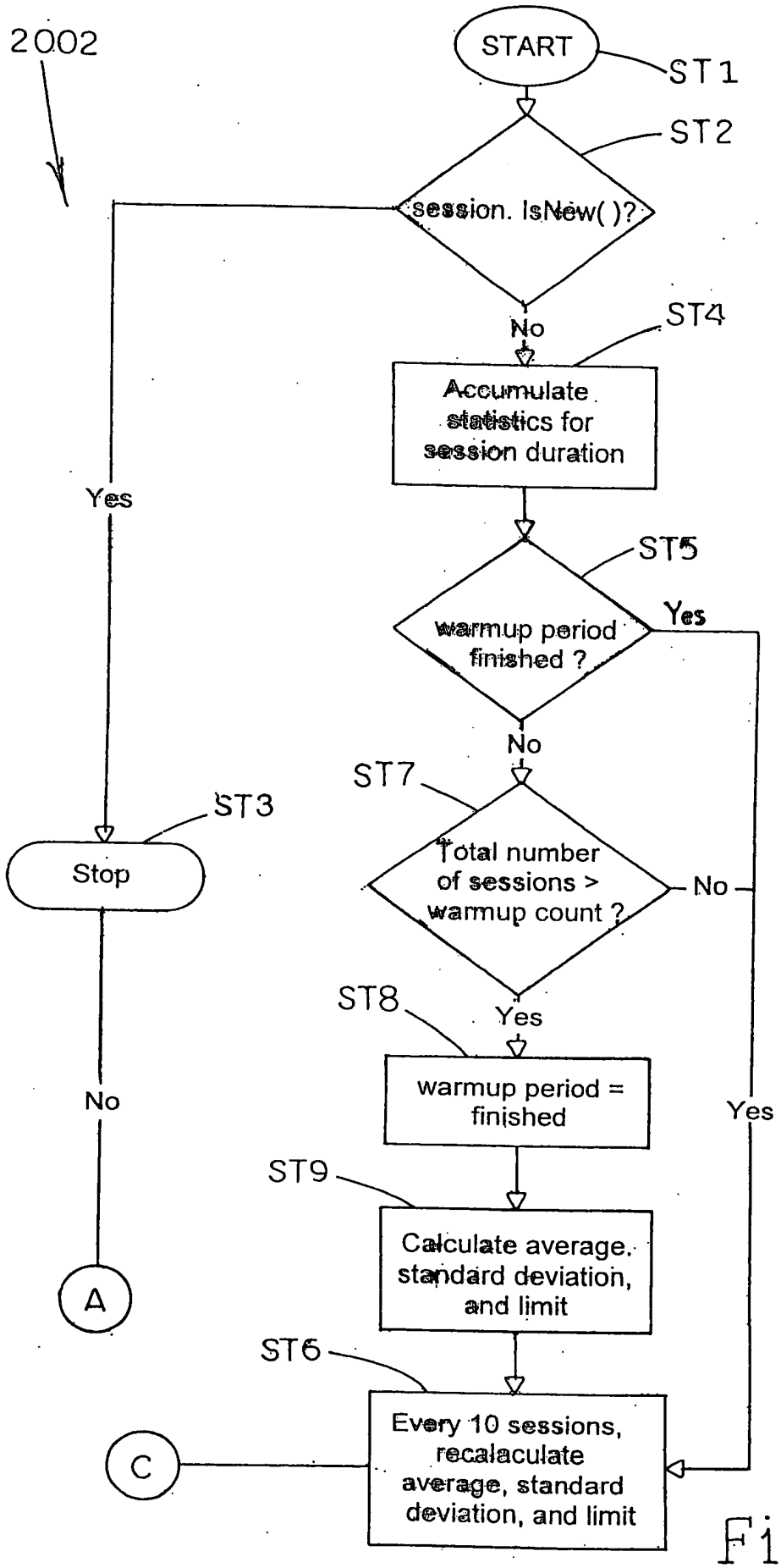
2002
START
ST1
ST2
session. IsNew( )?
No
ST4
Accumulate statistics for session duration
Yes
ST5
warmup period finished ?
Yes
No
ST7
Total number of sessions > warmup count ?
No
ST3
Stop
Yes
ST8
warmup period = finished
No
ST9
Calculate average, standard deviation, and limit
A
ST6
Every 10 sessions, recalaculate average, standard deviation, and limit
C

FIG. 20B

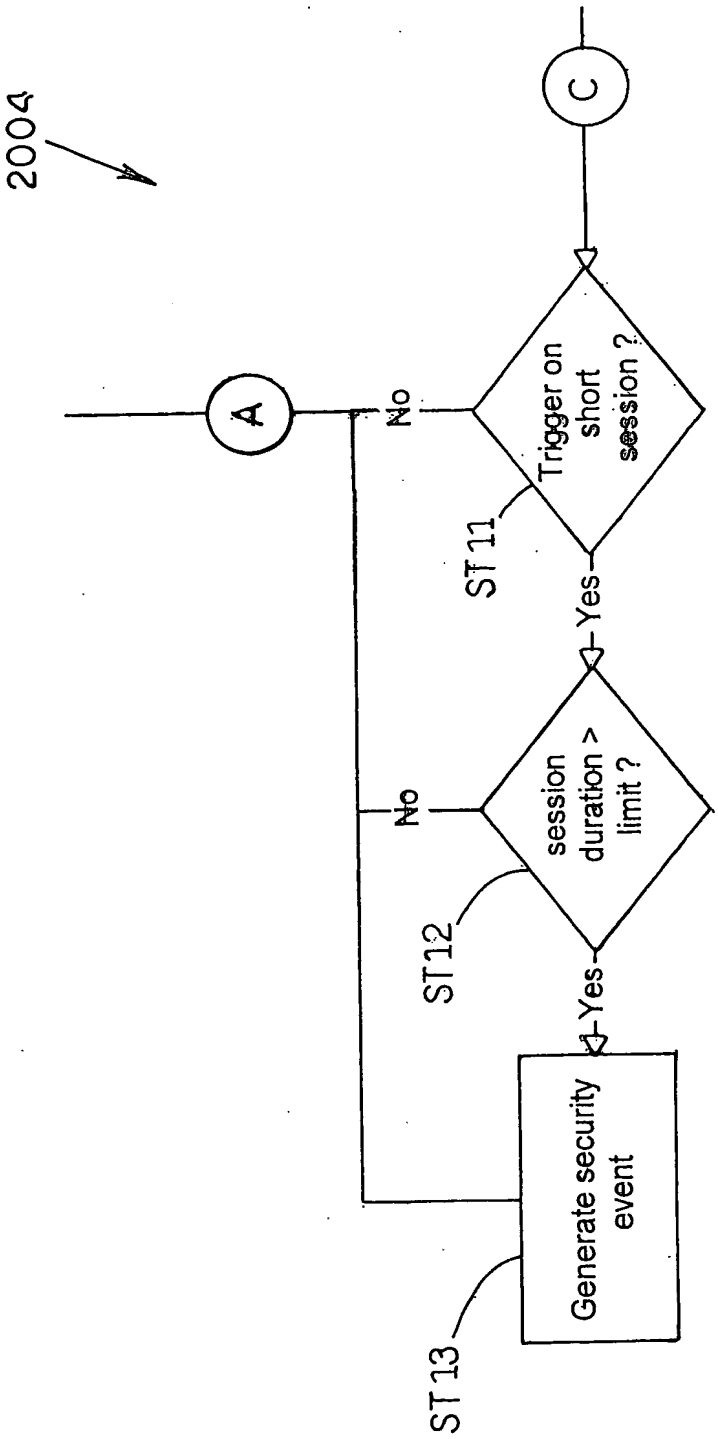
2004
A
C
No
Trigger on short session ?
ST 11
Yes
session duration > limit ?
No
ST12
Yes
Generate security event
ST 13

FIG. 20C

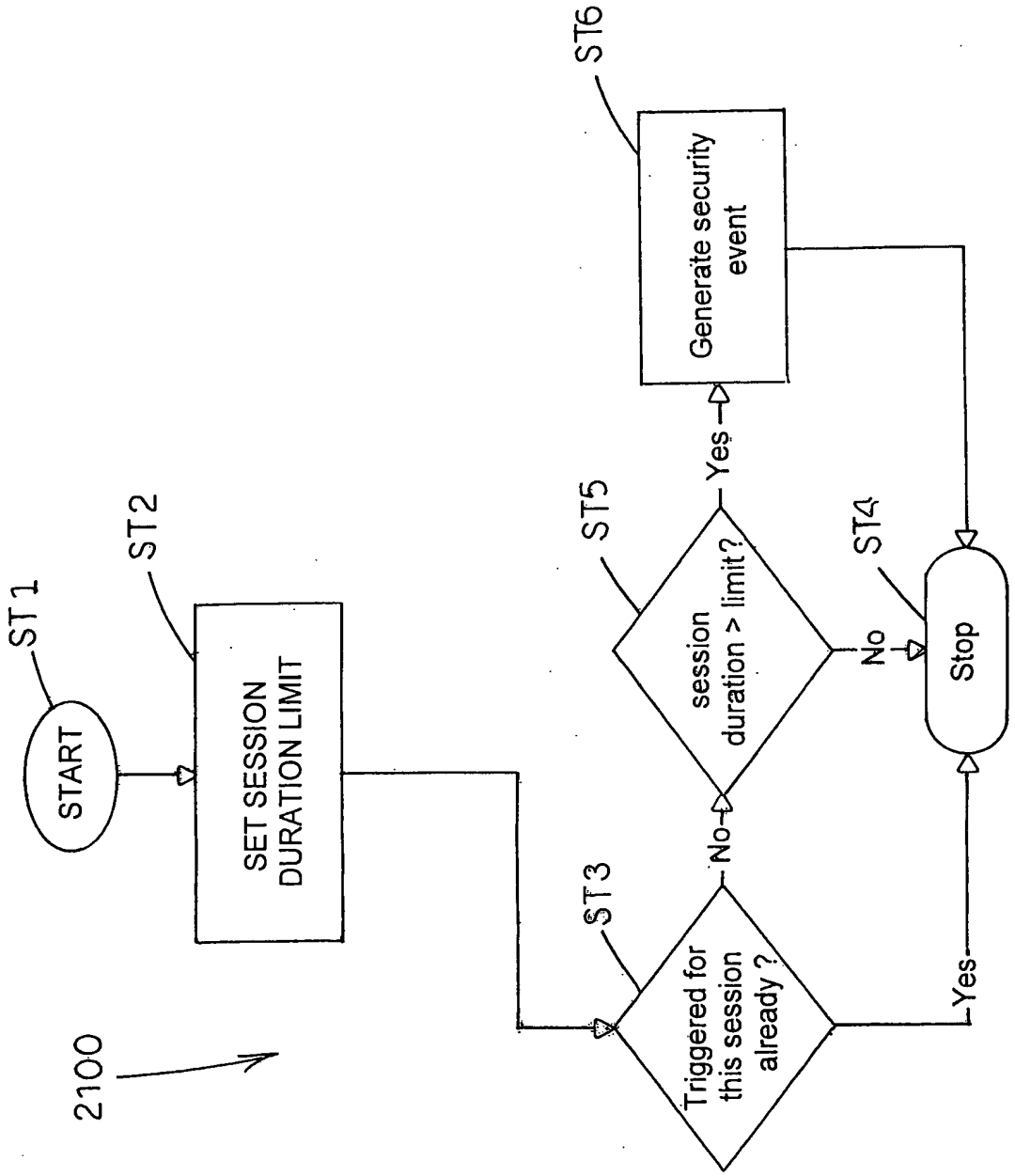
2100
START
ST1
SET SESSION DURATION LIMIT
ST2
Triggered for this session already ?
ST3
No
Yes
session duration > limit ?
ST5
Yes
No
Stop
ST4
Generate security event
ST6

Fig. 21

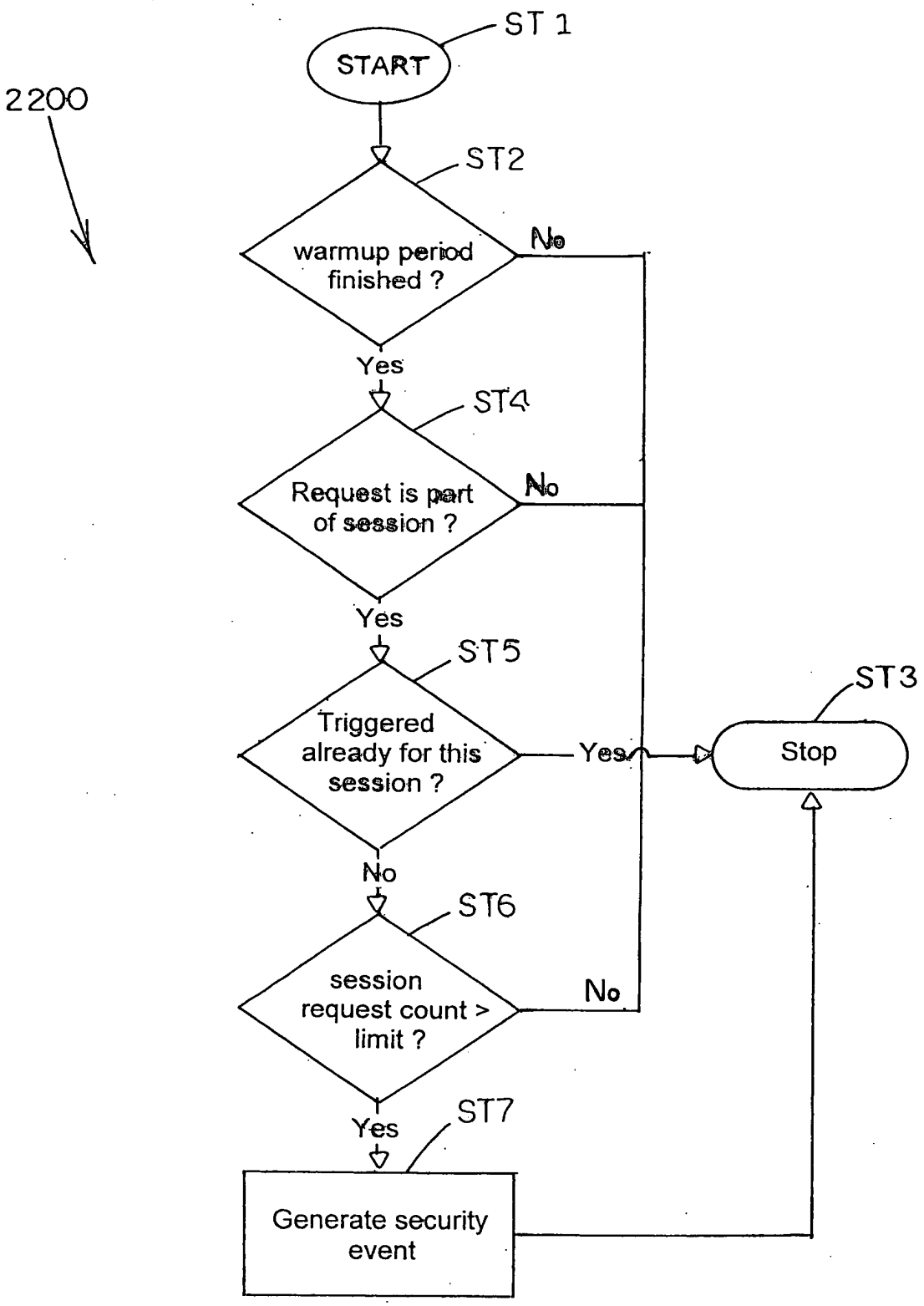
2200
START
ST 1
ST2
warmup period finished ?
No
Yes
ST4
Request is part of session ?
No
Yes
ST5
Triggered already for this session ?
Yes
ST3
Stop
No
ST6
session request count > limit ?
No
Yes
ST7
Generate security event

Fig. 22A

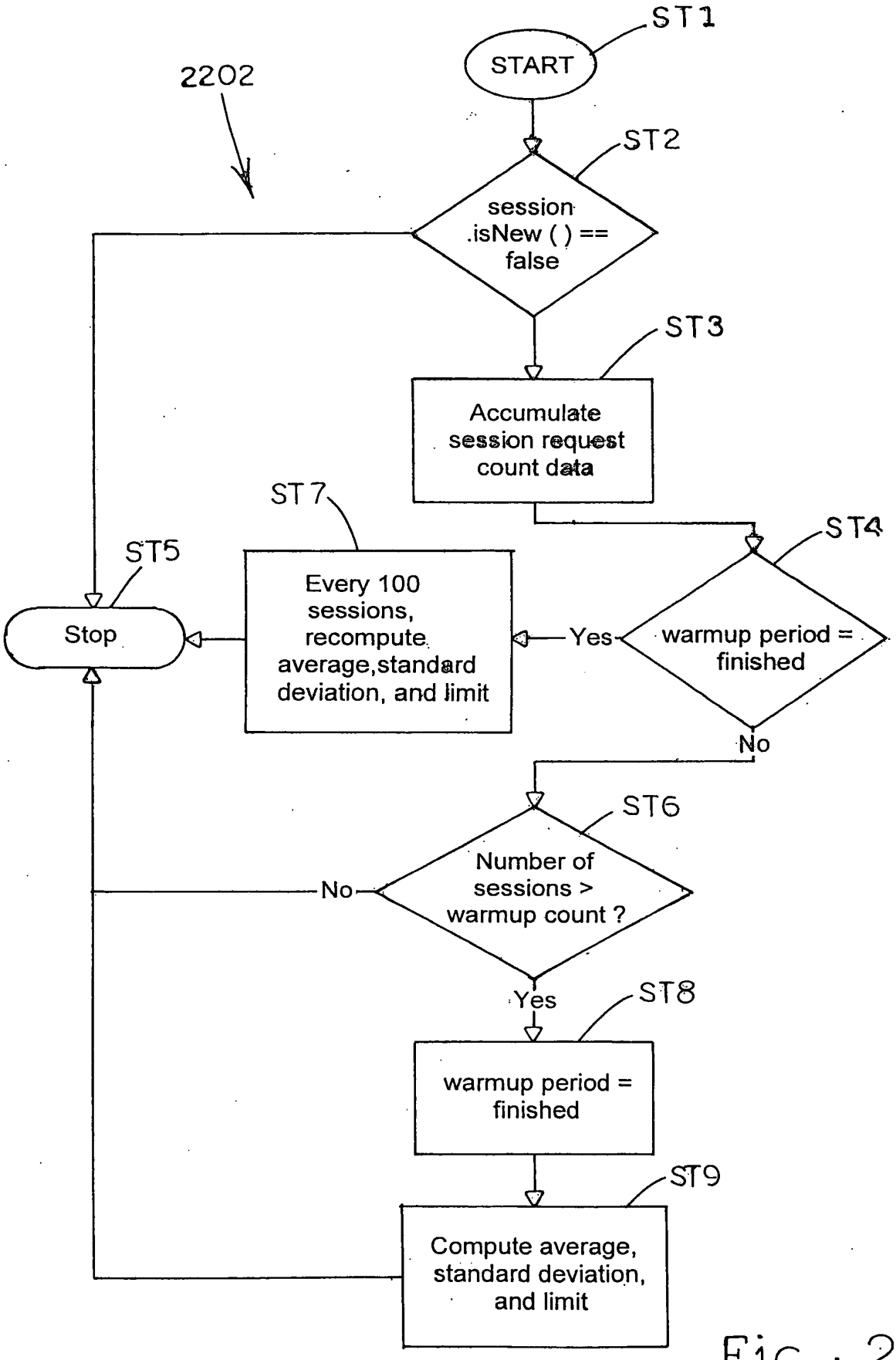
2202
START
ST1
ST2
session .isNew ( ) == false
ST3
Accumulate session request count data
ST4
warmup period = finished
Yes
No
ST5
Stop
ST6
Number of sessions > warmup count ?
No
Yes
ST7
Every 100 sessions, recompute average,standard deviation, and limit
ST8
warmup period = finished
ST9
Compute average, standard deviation, and limit

Fig. 22B

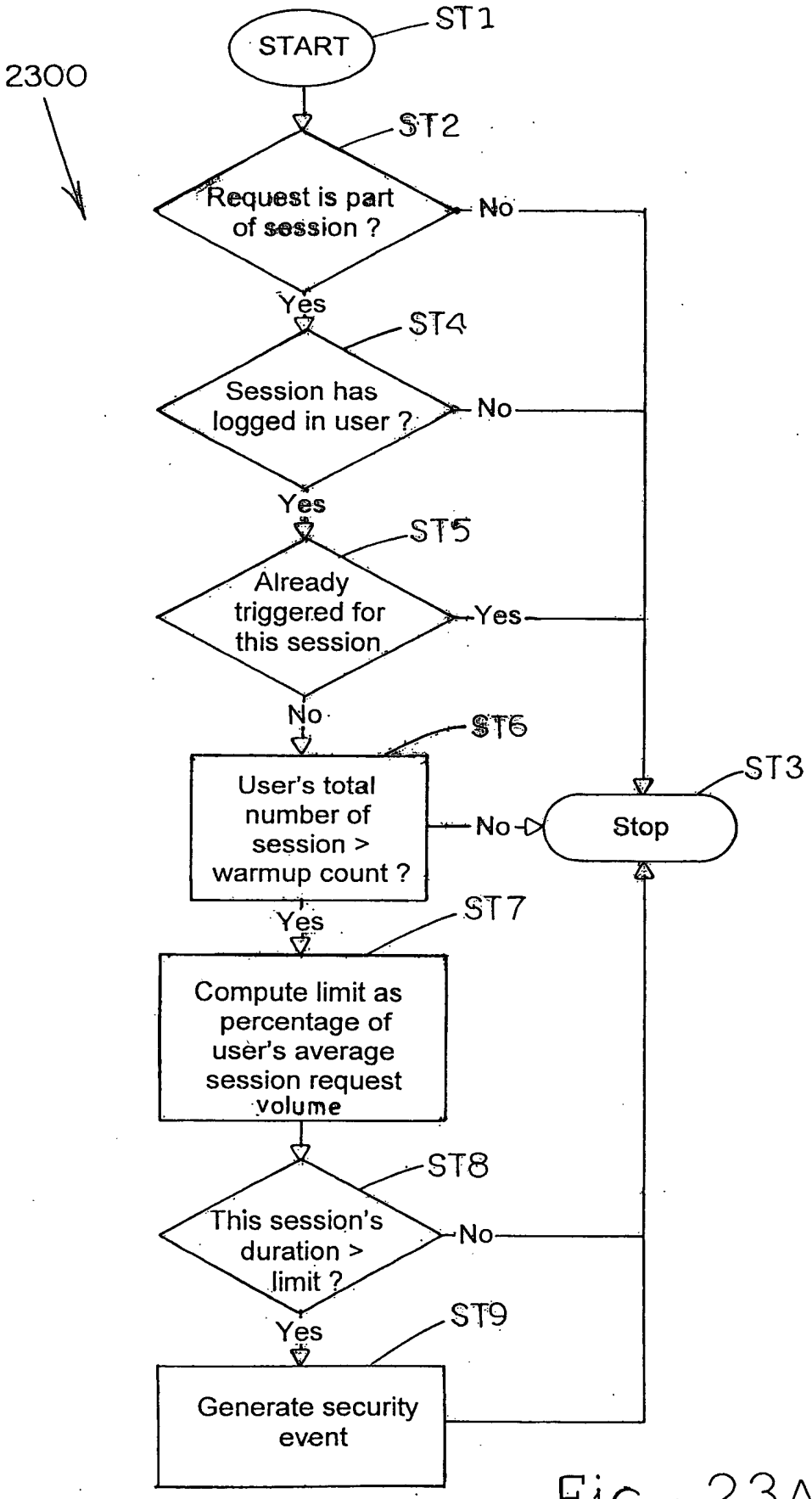
2300
START
ST1
ST2
Request is part of session ?
No
Yes
ST4
Session has logged in user ?
No
Yes
ST5
Already triggered for this session
Yes
No
ST6
User's total number of session > warmup count ?
No
ST3
Stop
Yes
ST7
Compute limit as percentage of user's average session request volume
ST8
This session's duration > limit ?
No
Yes
ST9
Generate security event

FIG. 23A

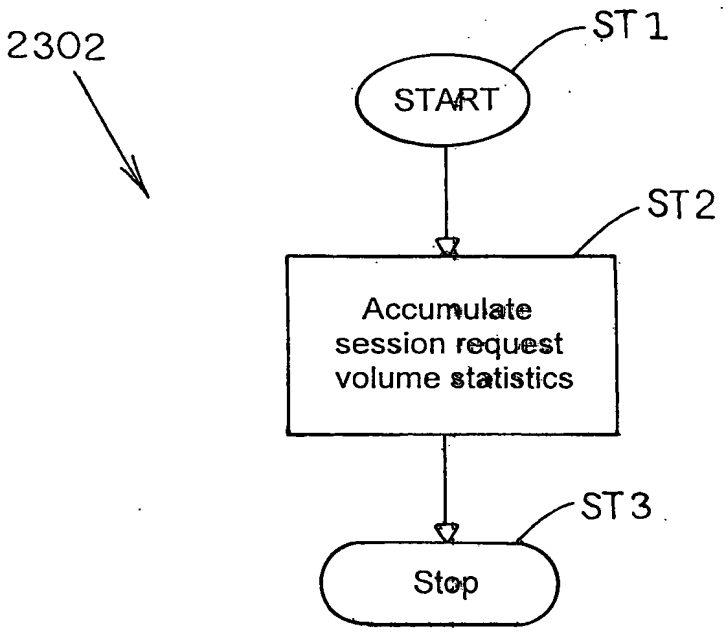
2302
ST1
START
ST2
Accumulate session request volume statistics
ST3
Stop

FIG. 23B

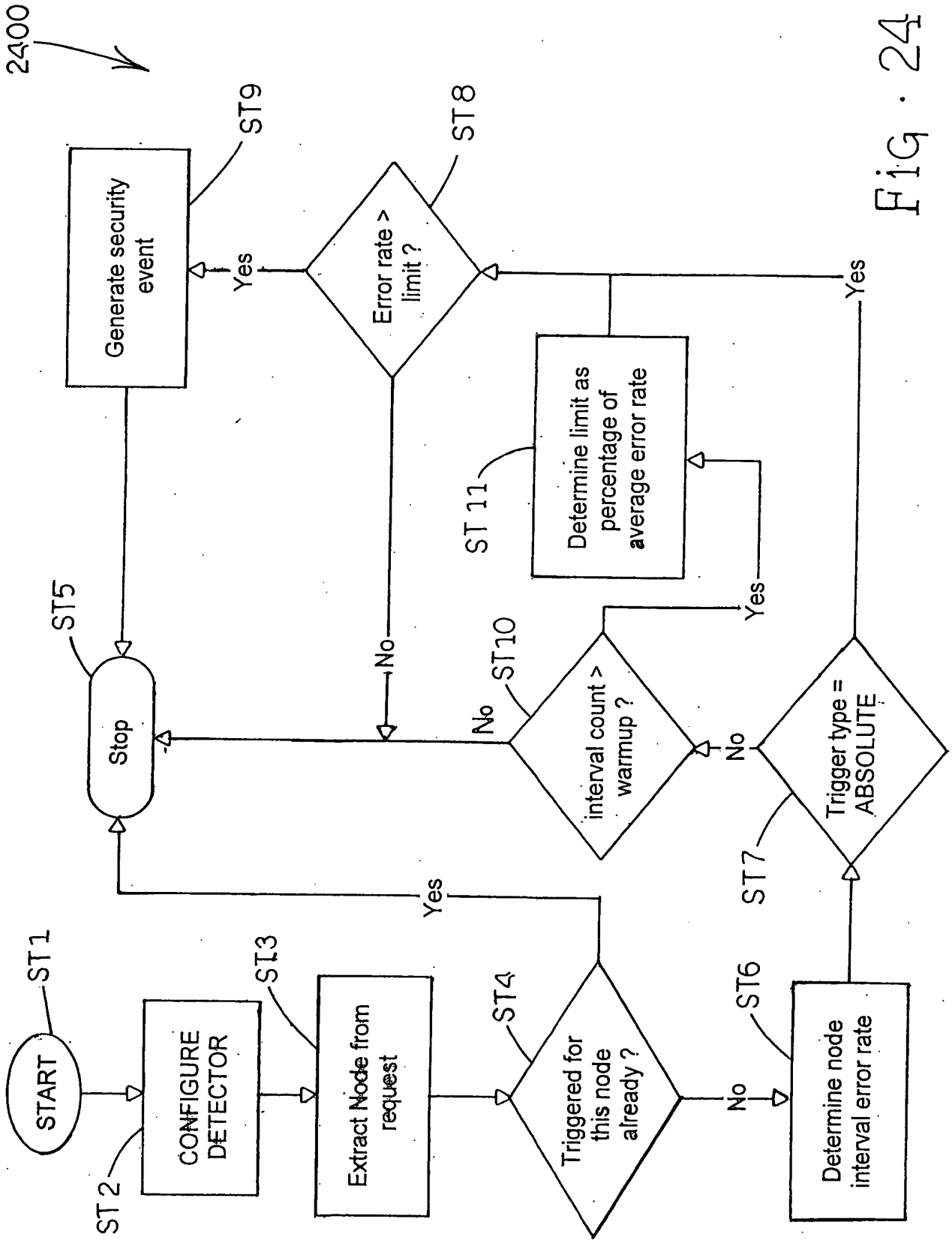
2400
START
ST1
CONFIGURE DETECTOR
ST2
ST3
Extract Node from request
ST4
Triggered for this node already ?
Yes
No
ST5
Stop
ST6
Determine node interval error rate
ST7
Trigger type = ABSOLUTE
No
Yes
ST10
interval count > warmup ?
No
Yes
ST11
Determine limit as percentage of average error rate
ST8
Error rate > limit ?
Yes
No
ST9
Generate security event

Fig. 24

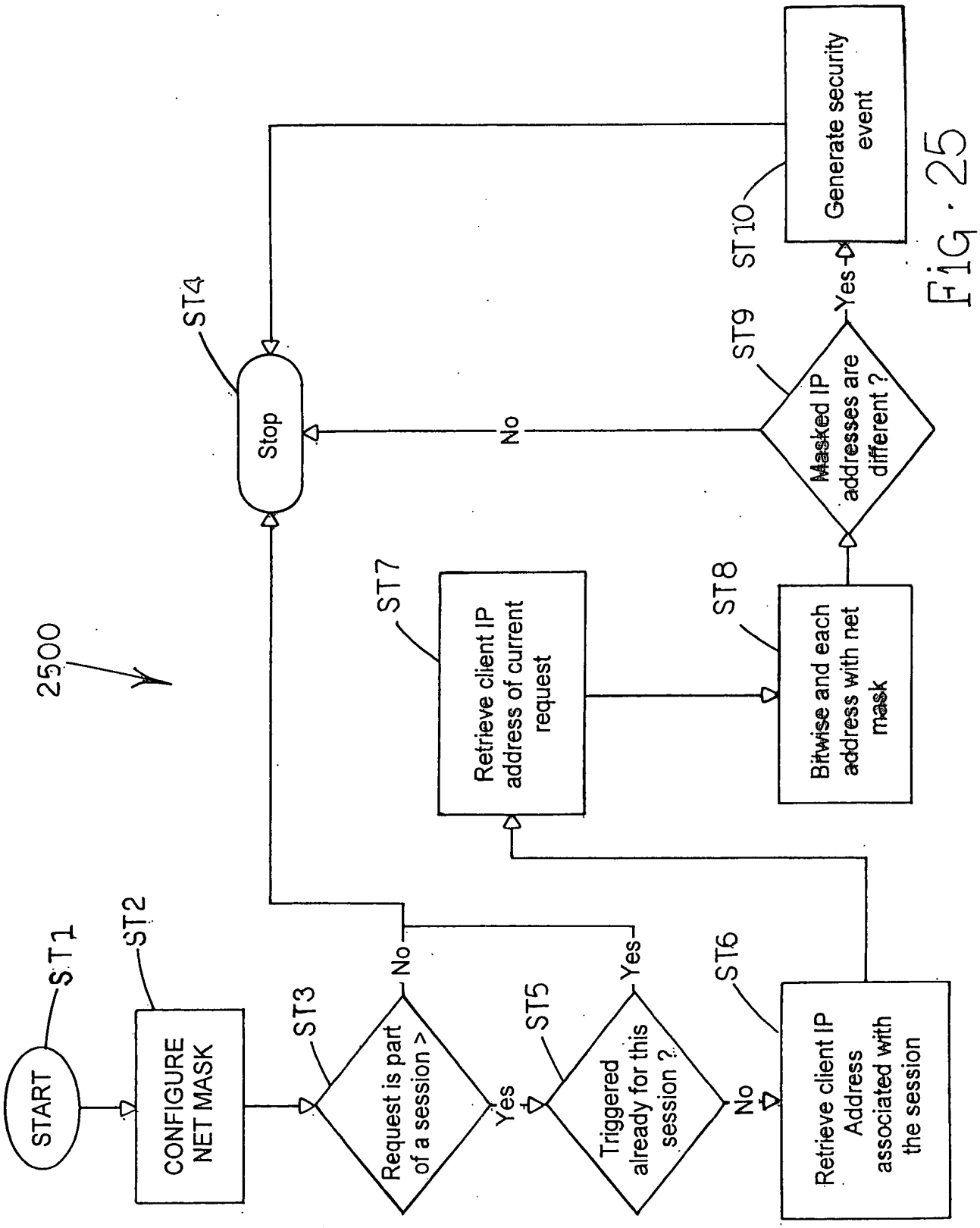
2500
START
ST1
CONFIGURE NET MASK
ST2
ST3
Request is part of a session >
No
Yes
ST5
Triggered already for this session ?
Yes
No
ST6
Retrieve client IP Address associated with the session
ST7
Retrieve client IP address of current request
ST8
Bitwise and each address with net mask
ST9
Masked IP addresses are different ?
Yes
No
ST10
Generate security event
ST4
Stop

FIG. 25

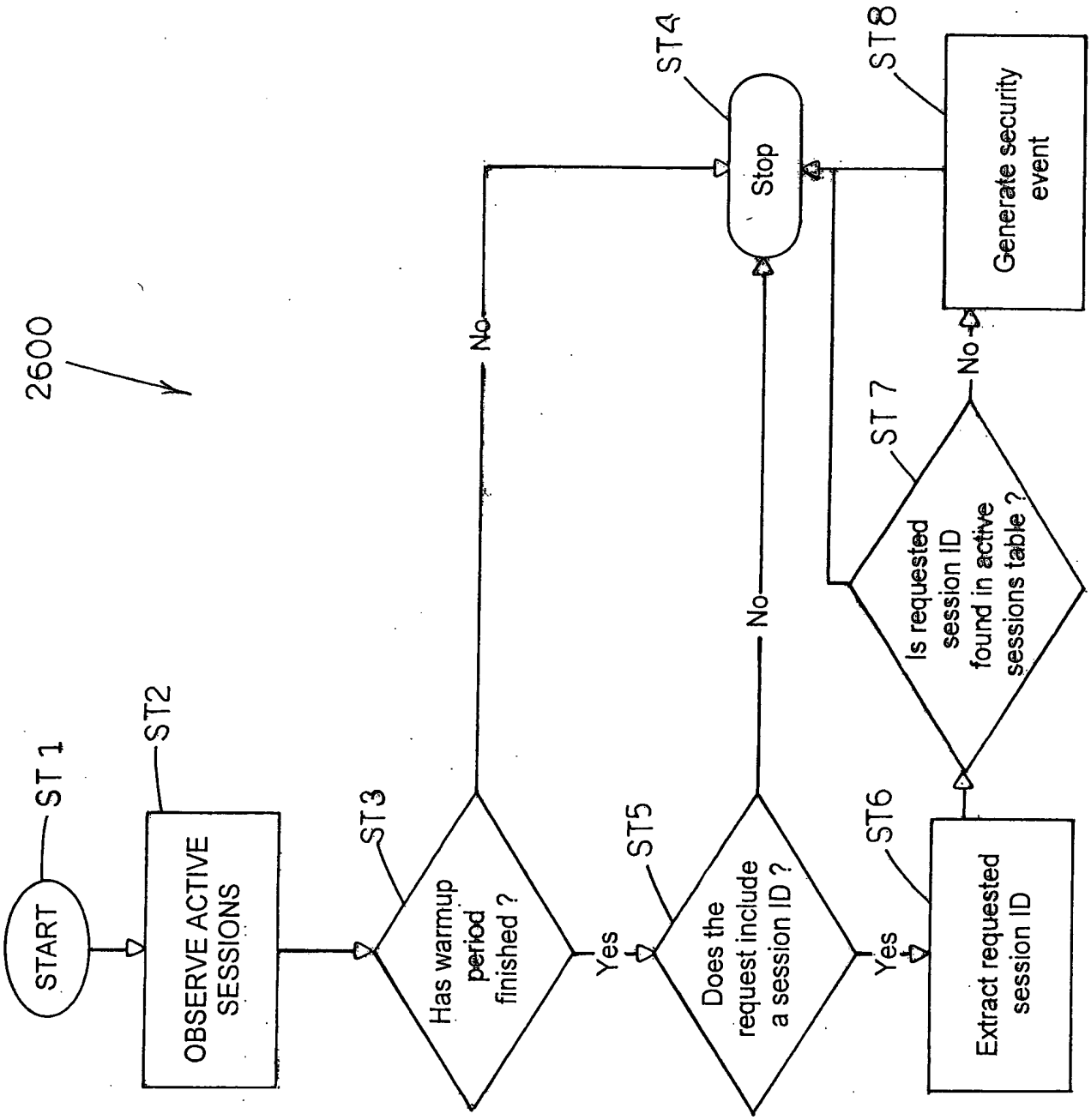
2600
START
ST 1
OBSERVE ACTIVE SESSIONS
ST2
Has warmup period finished ?
ST3
No
Yes
Does the request include a session ID ?
ST5
No
Yes
Is requested session ID found in active sessions table ?
ST 7
No
Extract requested session ID
ST6
Generate security event
ST8
Stop
ST4

FIG. 26

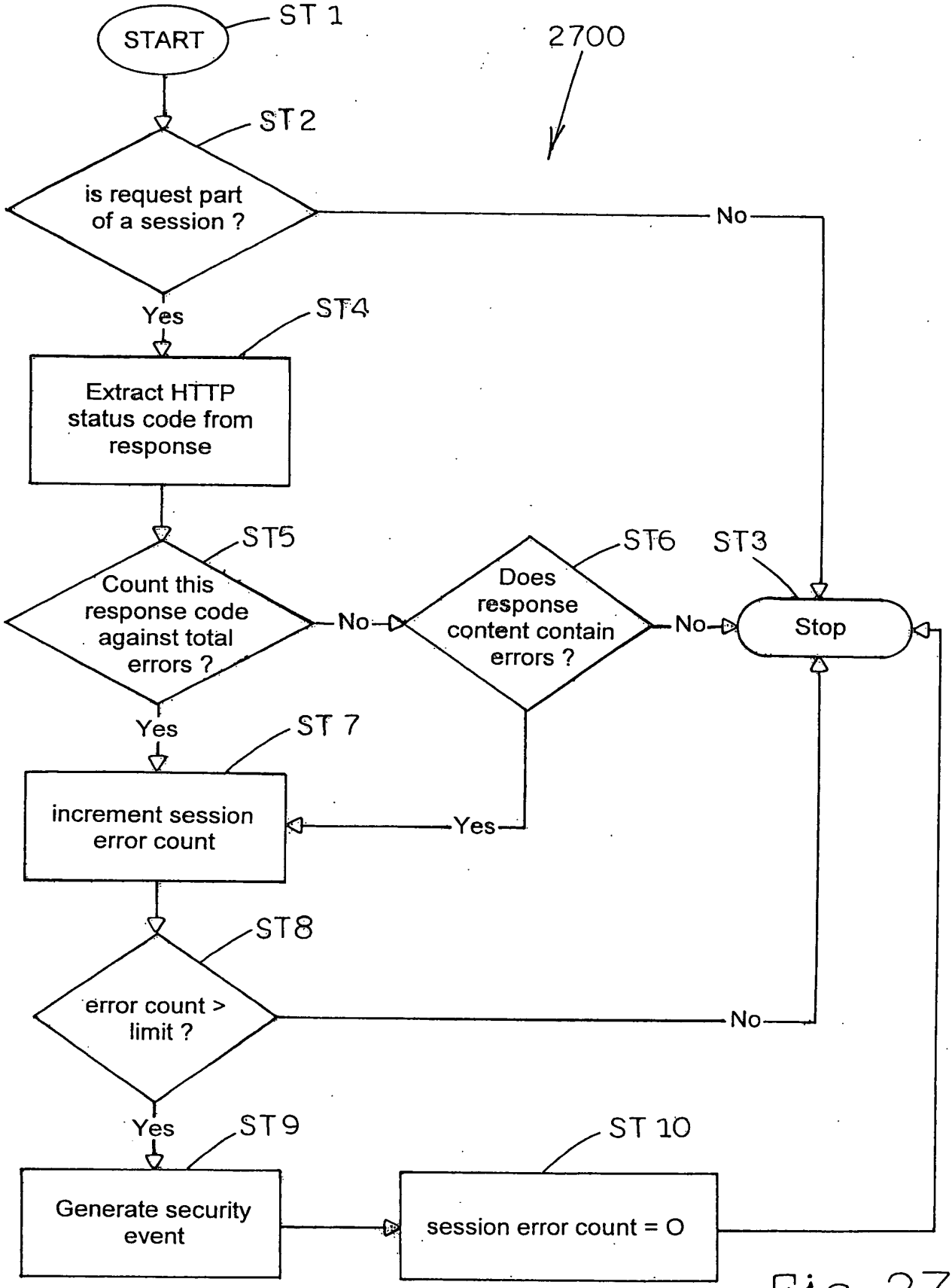
START
ST 1
2700
ST2
is request part of a session ?
No
Yes
ST4
Extract HTTP status code from response
ST5
Count this response code against total errors ?
No
ST6
Does response content contain errors ?
No
ST3
Stop
Yes
ST 7
increment session error count
Yes
ST8
error count > limit ?
No
Yes
ST 9
Generate security event
ST 10
session error count = O

Fig. 27

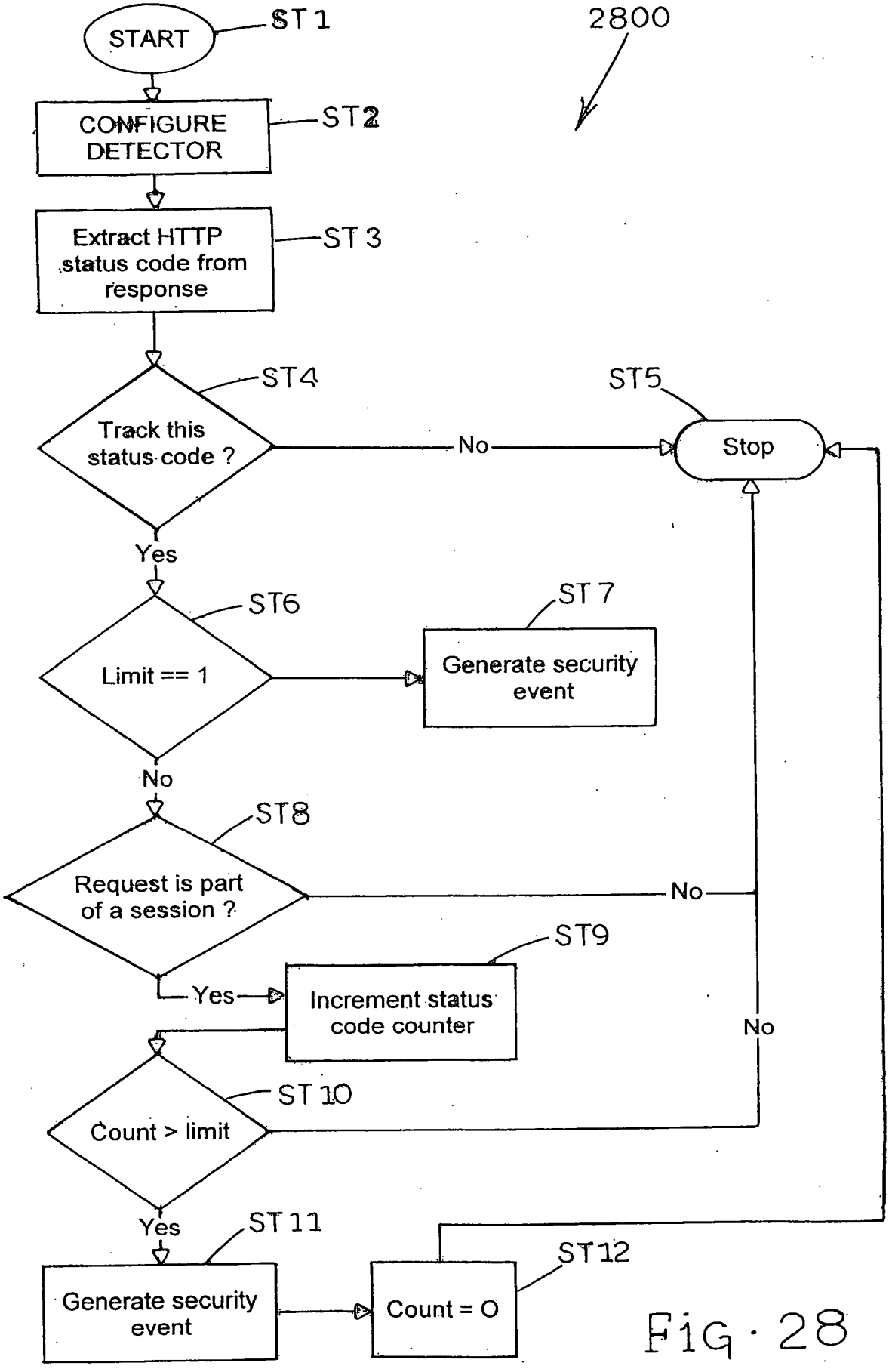
START
ST 1
2800
CONFIGURE DETECTOR
ST2
Extract HTTP status code from response
ST 3
Track this status code ?
ST4
No
ST5
Stop
Yes
Limit == 1
ST6
Generate security event
ST 7
No
Request is part of a session ?
ST8
No
Yes
Increment status code counter
ST9
No
Count > limit
ST 10
Yes
Generate security event
ST 11
Count = 0
ST12

Fig. 28

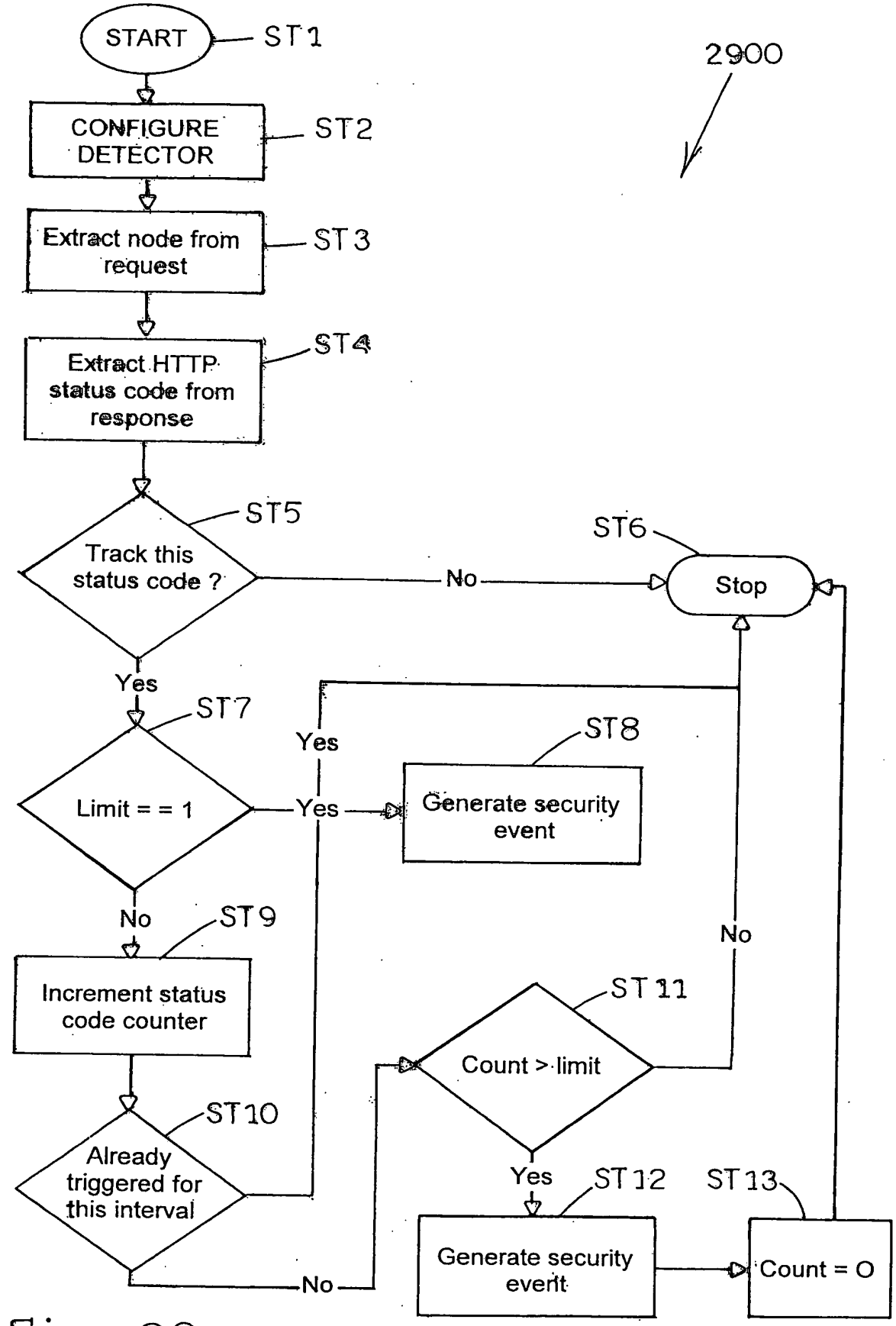
START
ST1
2900
CONFIGURE DETECTOR
ST2
Extract node from request
ST3
Extract HTTP status code from response
ST4
Track this status code ?
ST5
No
ST6
Stop
Yes
ST7
Limit = = 1
Yes
Yes
ST8
Generate security event
No
ST9
Increment status code counter
ST10
Already triggered for this interval
No
ST11
Count > limit
No
Yes
ST12
Generate security event
ST13
Count = O

Fig. 29

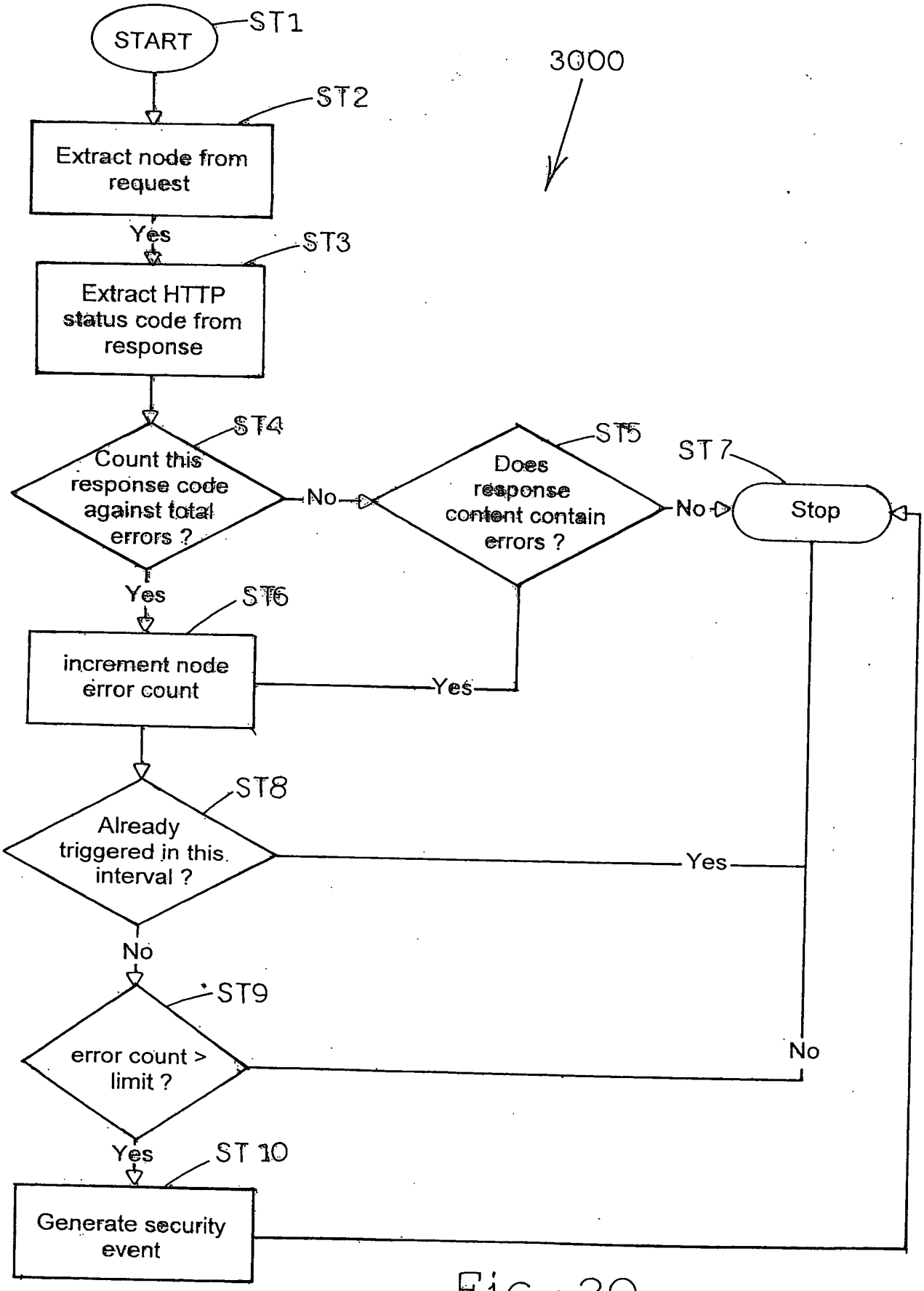
START
ST1
3000
ST2
Extract node from request
Yes
ST3
Extract HTTP status code from response
ST4
Count this response code against total errors ?
No
ST5
Does response content contain errors ?
ST7
No
Stop
Yes
ST6
increment node error count
Yes
ST8
Already triggered in this interval ?
Yes
No
ST9
error count > limit ?
No
Yes
ST 10
Generate security event

Fig. 30

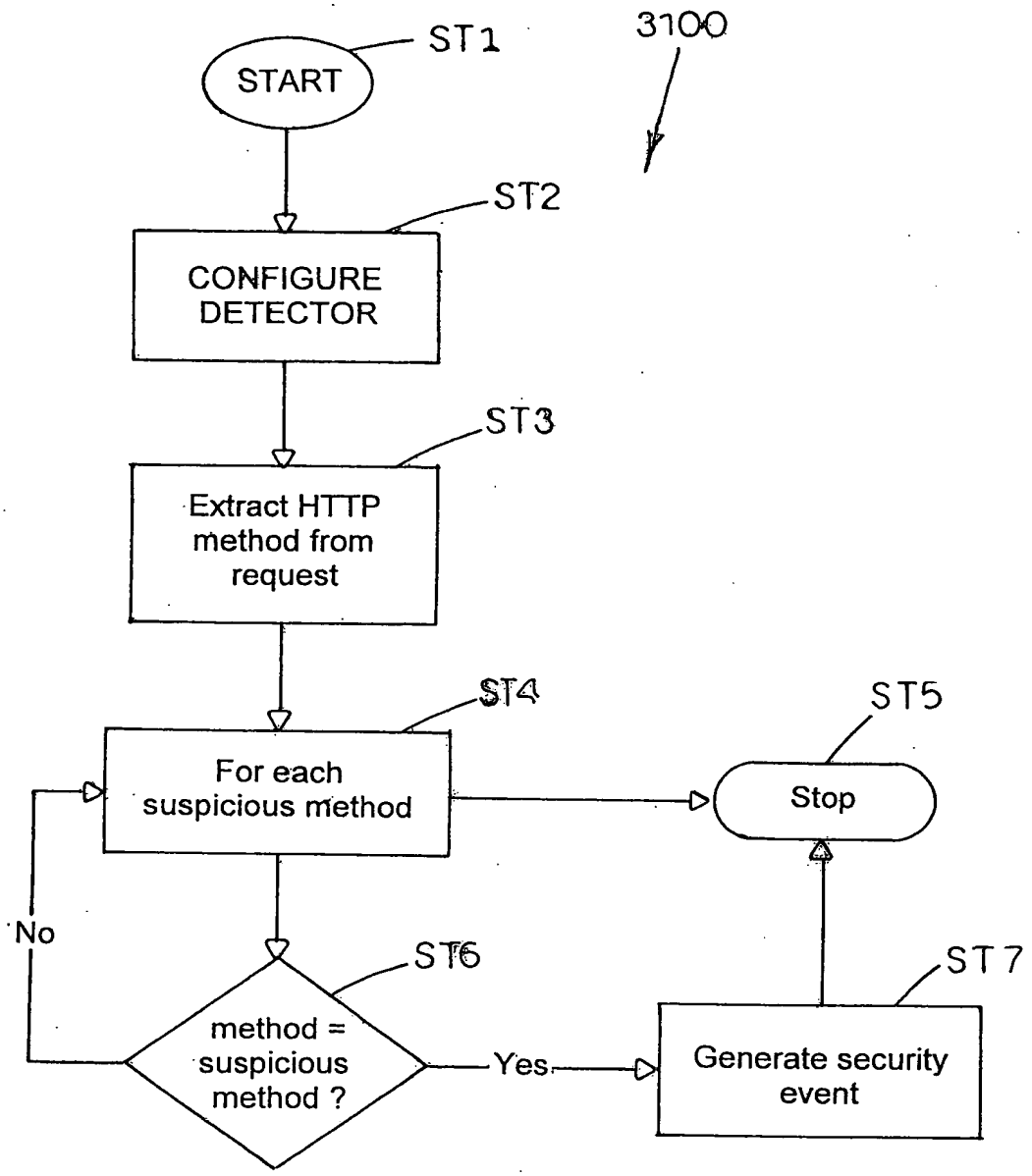
3100
ST1
START
ST2
CONFIGURE DETECTOR
ST3
Extract HTTP method from request
ST4
For each suspicious method
ST5
Stop
No
ST6
method = suspicious method ?
Yes
ST7
Generate security event

Fig. 31

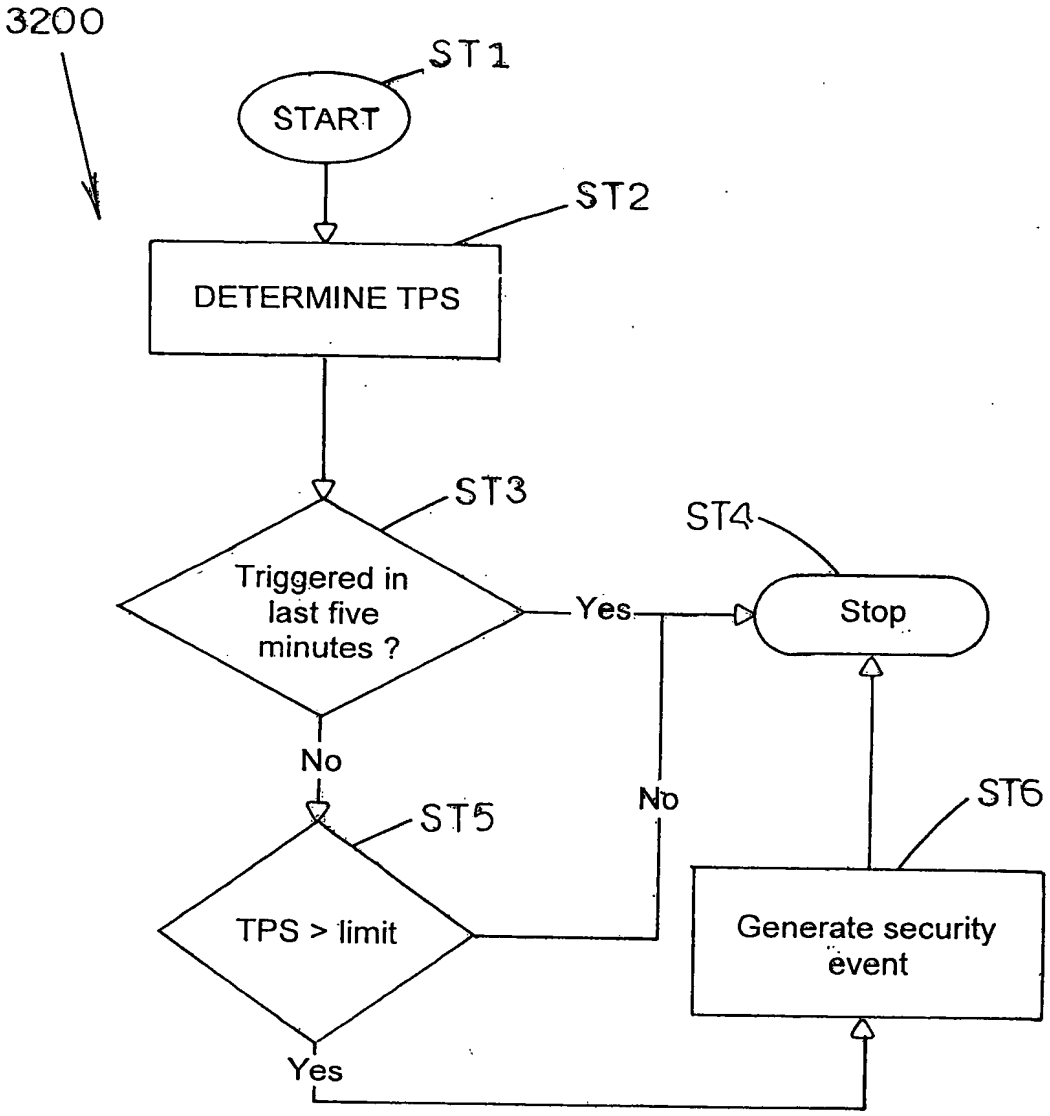
3200
ST1
START
ST2
DETERMINE TPS
ST3
Triggered in last five minutes ?
Yes
ST4
Stop
No
ST5
TPS > limit
No
ST6
Generate security event
Yes

Fig. 32

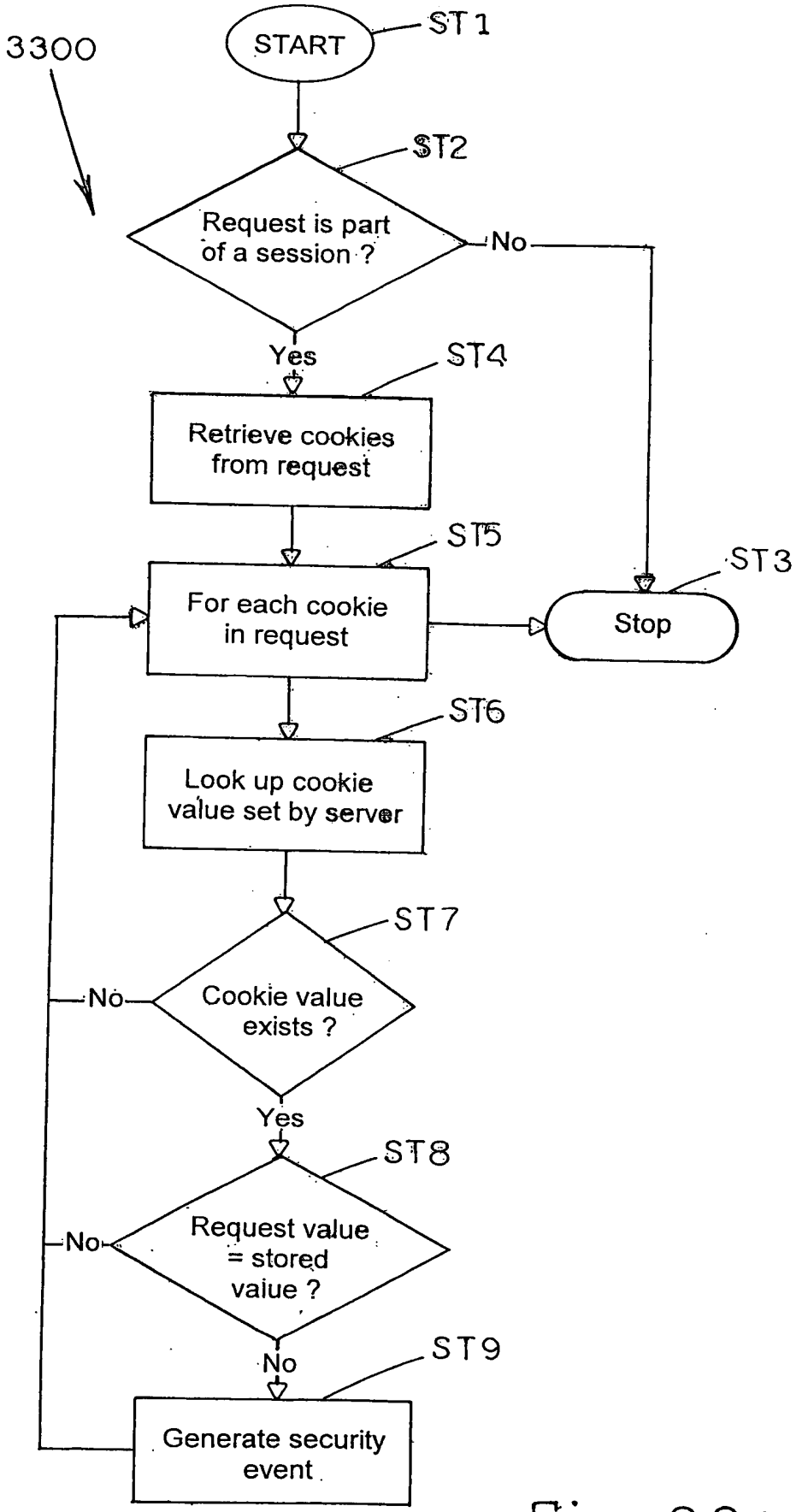
3300
START
ST1
ST2
Request is part of a session ?
No
Yes
ST4
Retrieve cookies from request
ST5
For each cookie in request
ST3
Stop
ST6
Look up cookie value set by server
ST7
No
Cookie value exists ?
Yes
ST8
No
Request value = stored value ?
No
ST9
Generate security event

FIG. 33A

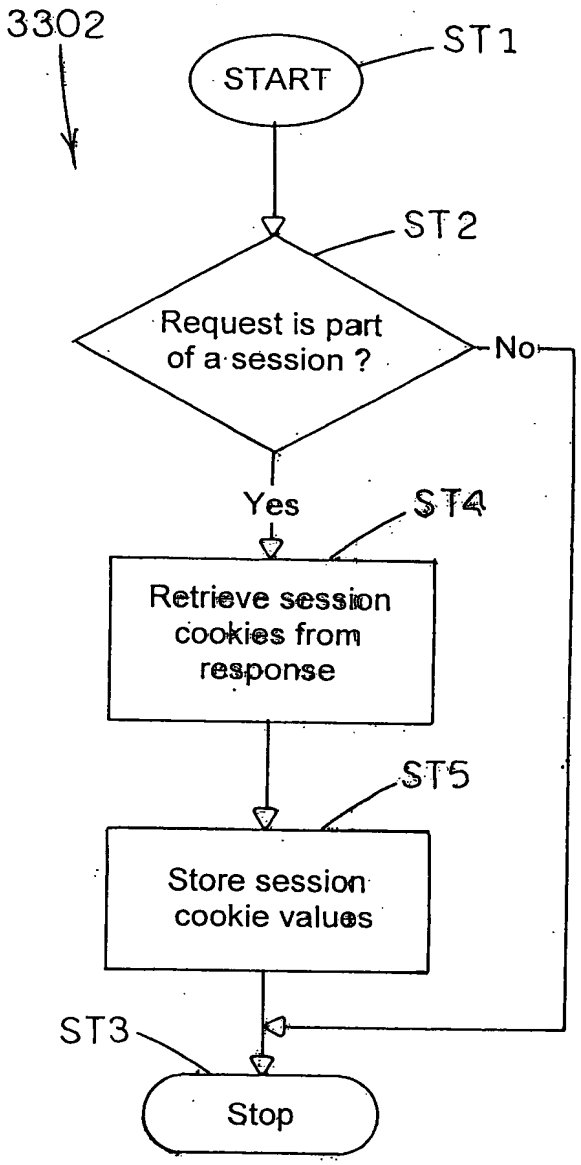
3302
START
ST1
ST2
Request is part of a session ?
No
Yes
ST4
Retrieve session cookies from response
ST5
Store session cookie values
ST3
Stop

FIG. 33B

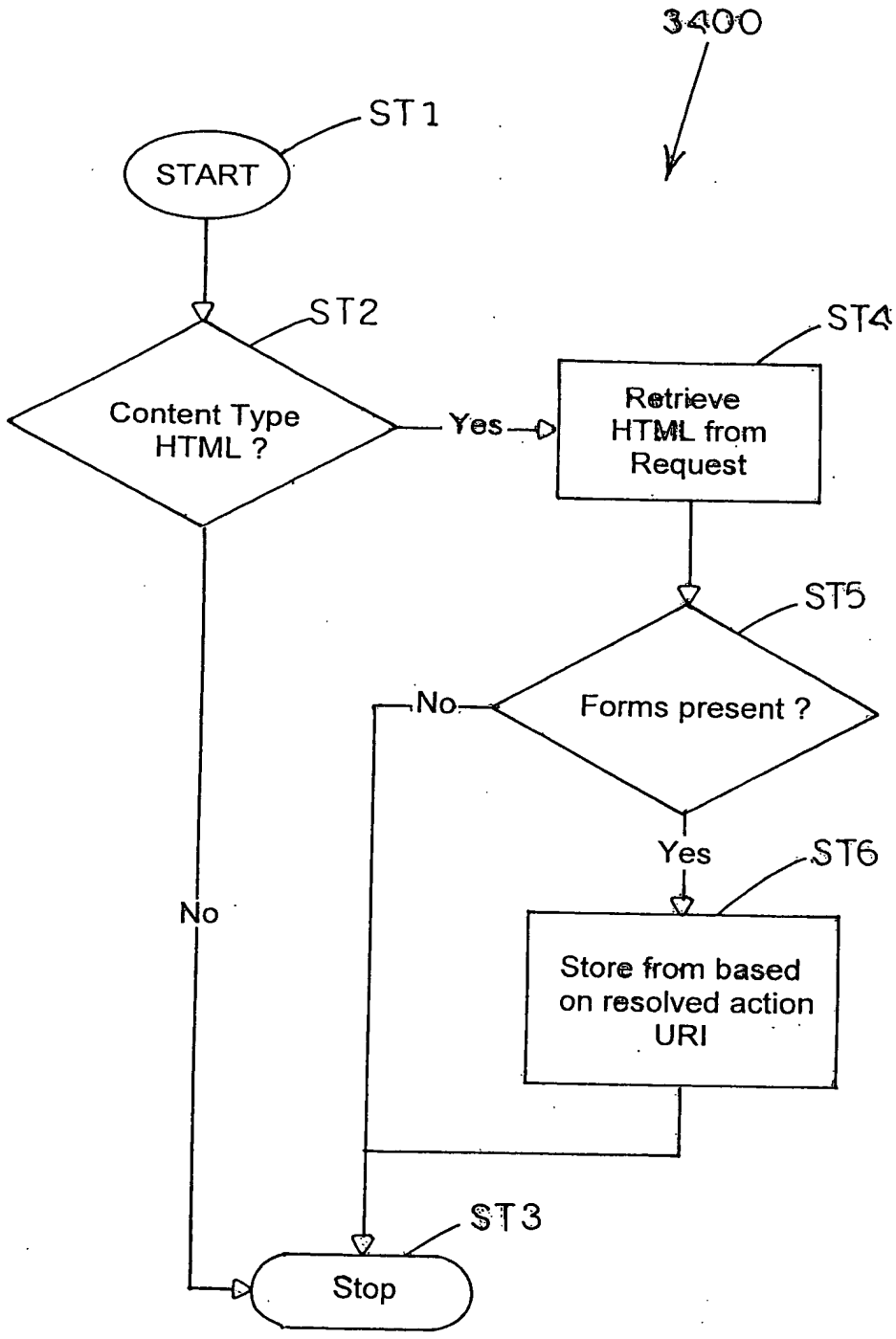
3400
ST1
START
ST2
Content Type HTML ?
Yes
ST4
Retrieve HTML from Request
ST5
Forms present ?
No
Yes
ST6
Store from based on resolved action URI
No
ST3
Stop

FIG. 34A

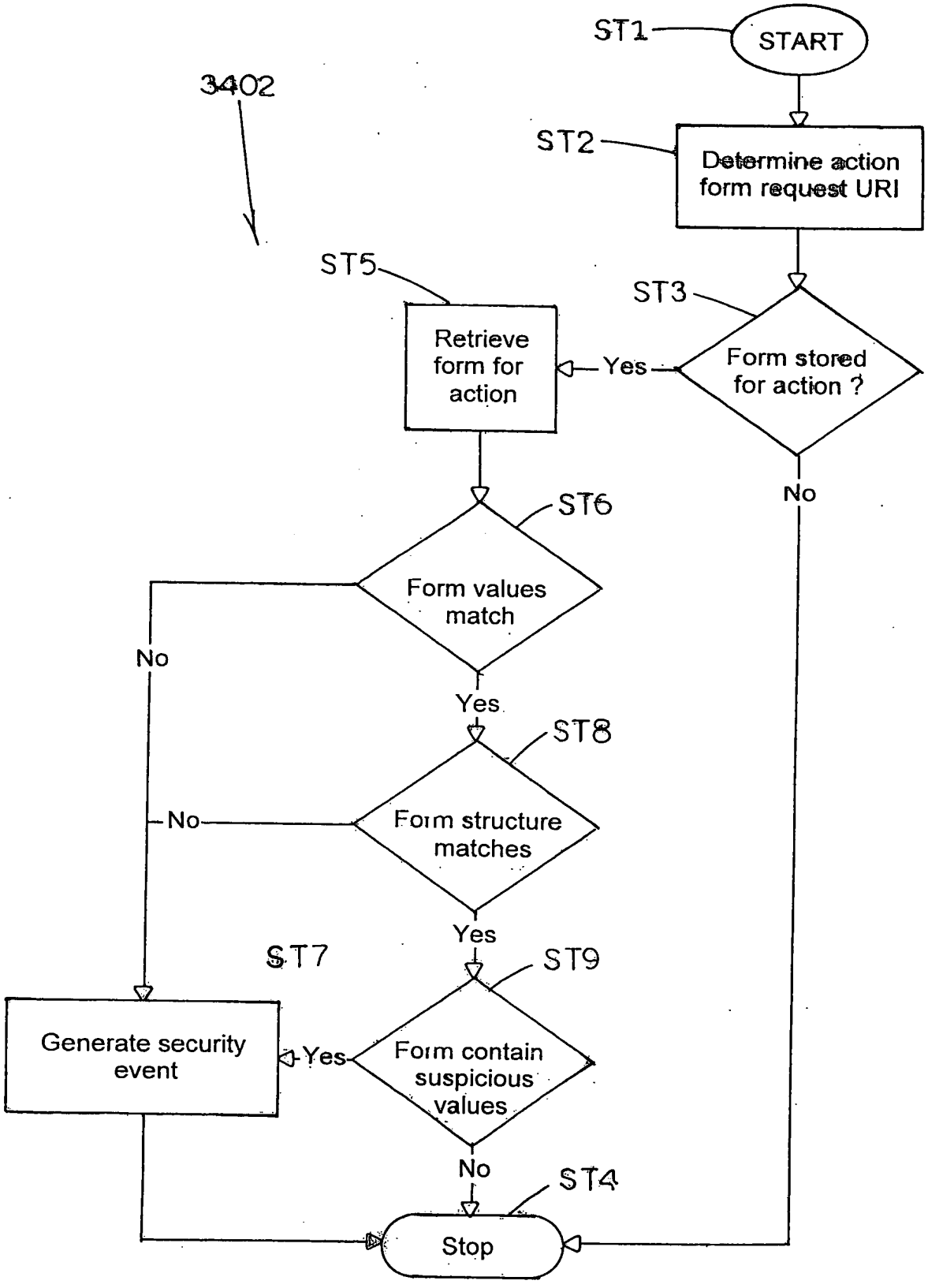
3402
ST1
START
ST2
Determine action form request URI
ST3
Form stored for action ?
Yes
No
ST5
Retrieve form for action
ST6
Form values match
No
Yes
ST8
Form structure matches
No
Yes
ST7
ST9
Generate security event
Yes
Form contain suspicious values
No
ST4
Stop

FIG · 34B

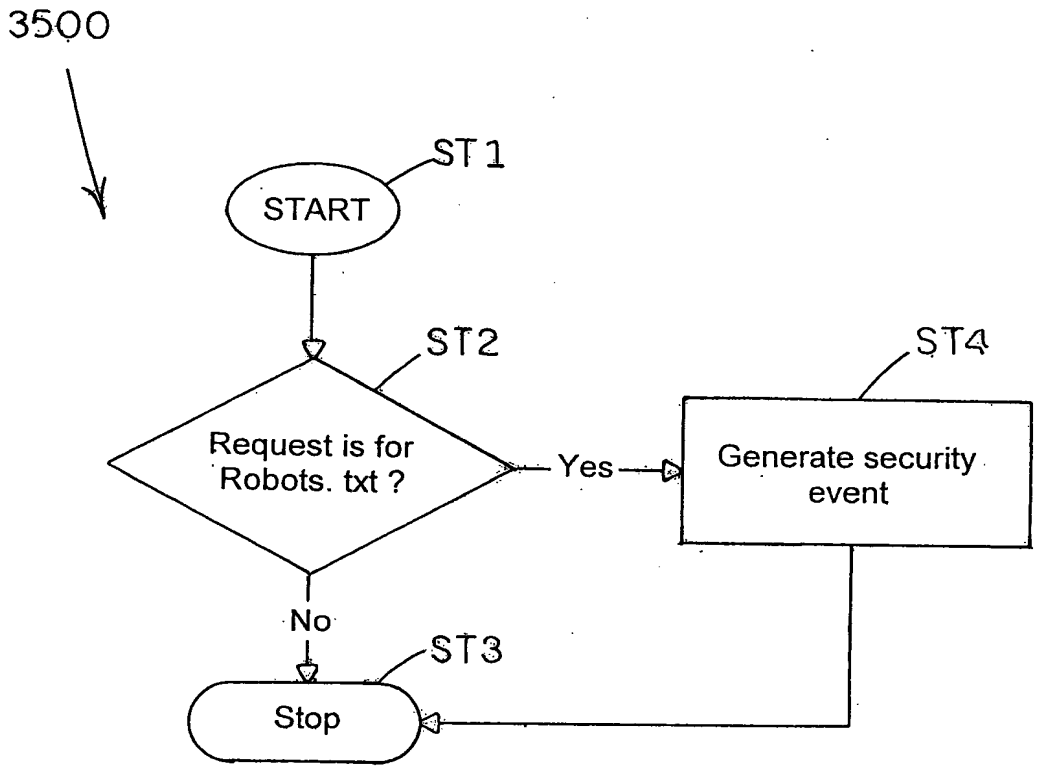
3500
ST1
START
ST2
Request is for Robots. txt ?
Yes
ST4
Generate security event
No
ST3
Stop

Fig. 35

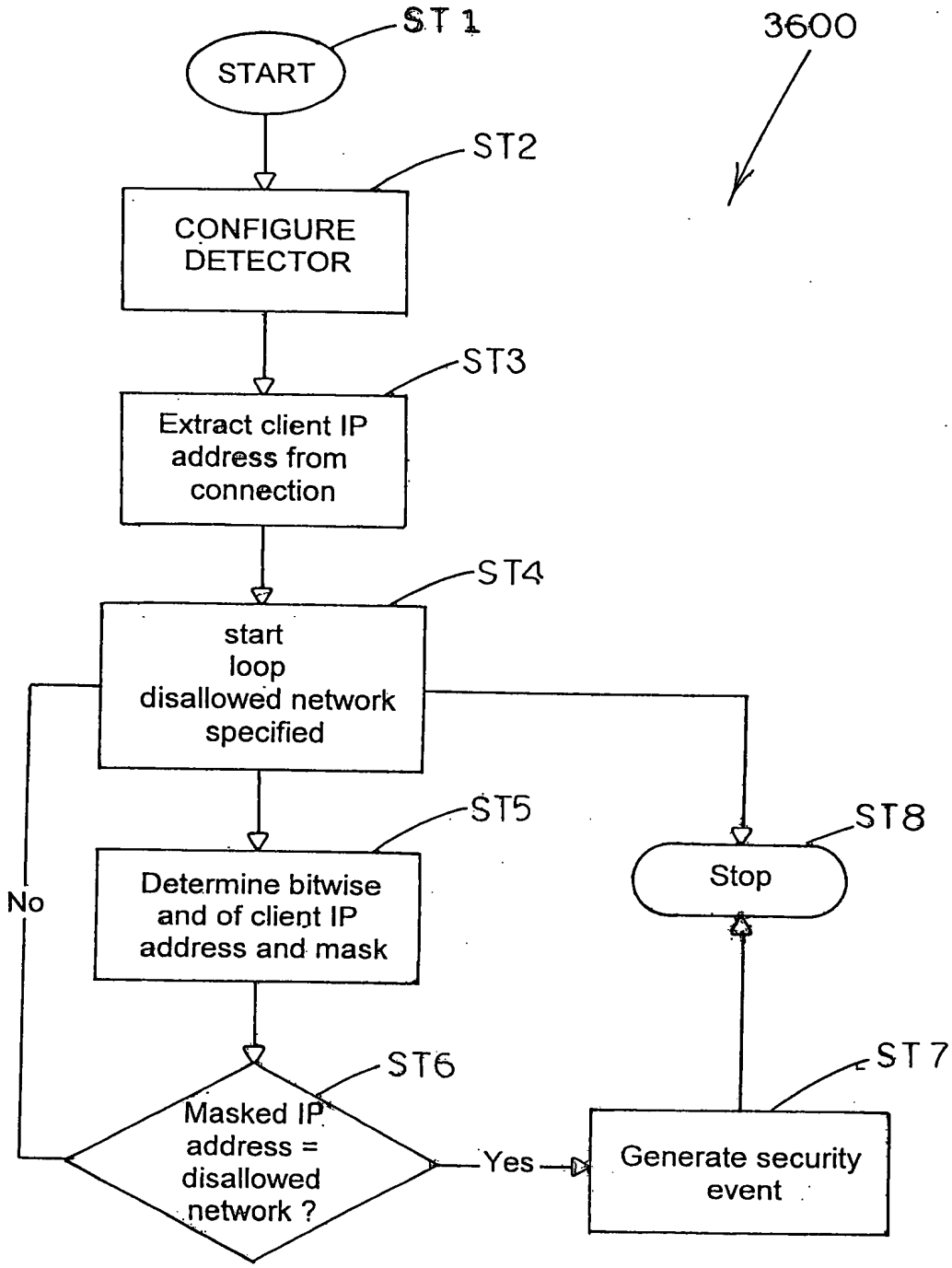
ST 1
START
3600
ST2
CONFIGURE DETECTOR
ST3
Extract client IP address from connection
ST4
start loop disallowed network specified
ST5
Determine bitwise and of client IP address and mask
ST6
Masked IP address = disallowed network ?
No
Yes
ST8
Stop
ST 7
Generate security event

Fig. 36

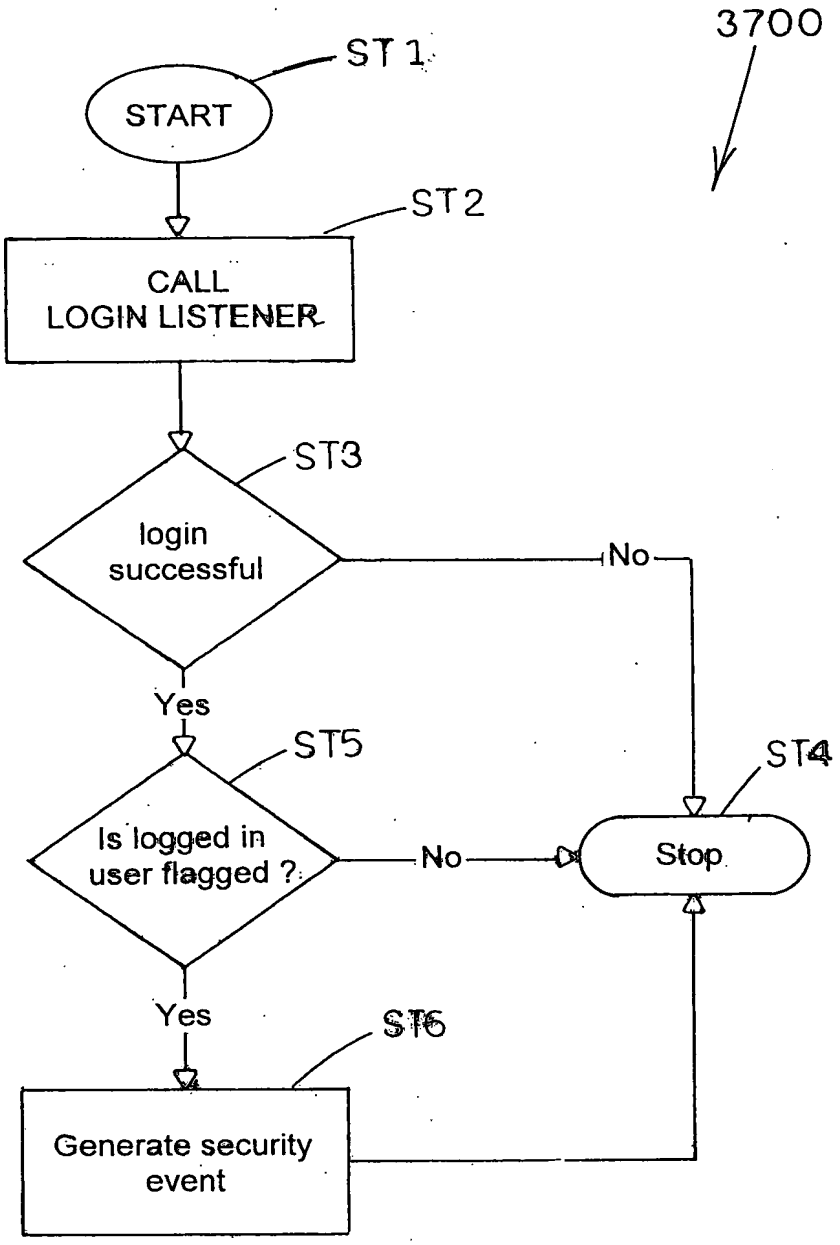
3700
ST 1
START
ST2
CALL
LOGIN LISTENER
ST3
login
successful
No
Yes
ST5
ST4
Is logged in
user flagged ?
No
Stop
Yes
ST6
Generate security
event

Fig. 37

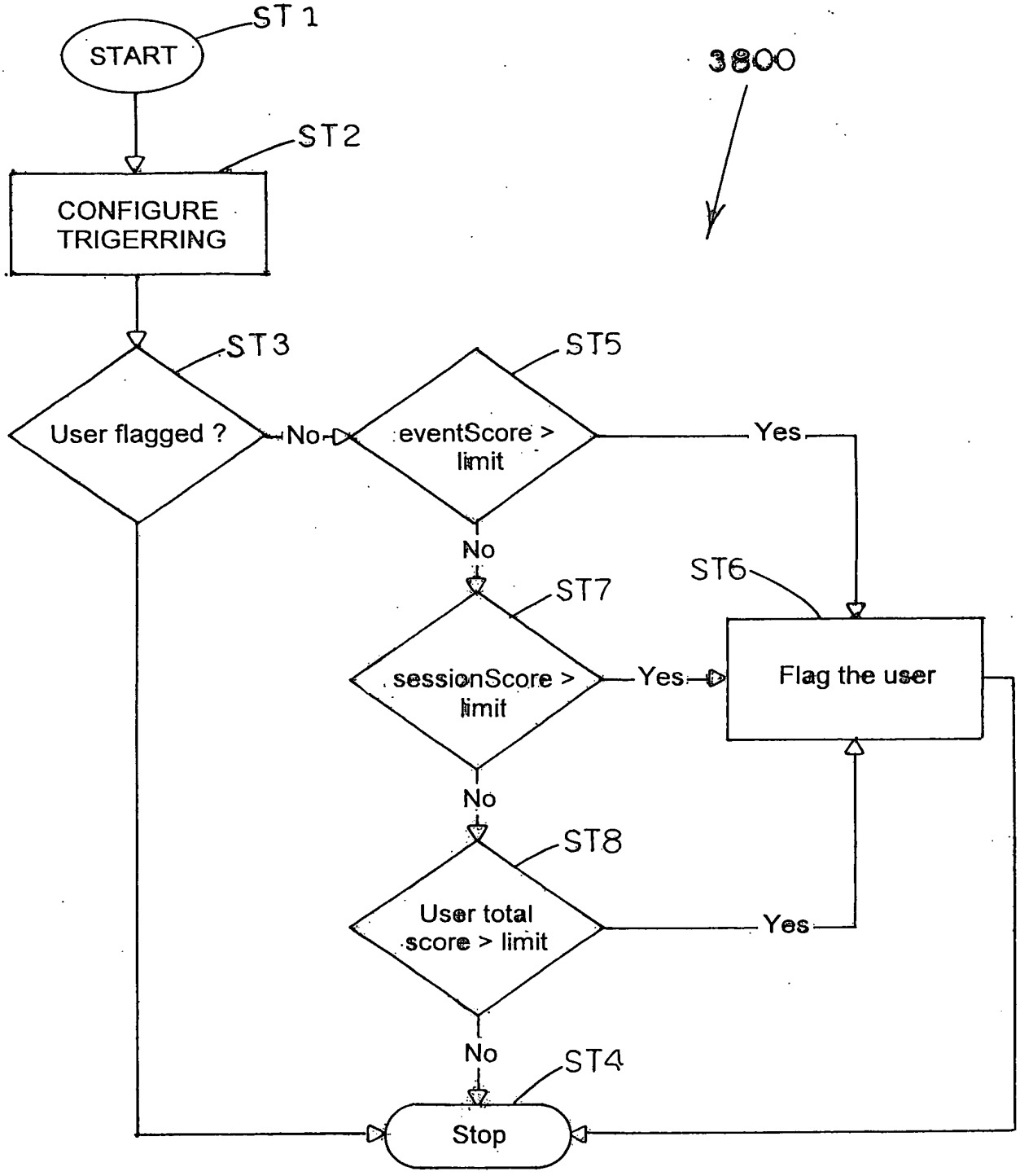
ST 1
START
3800
ST2
CONFIGURE TRIGERRING
ST3
User flagged ?
No
ST5
eventScore > limit
Yes
No
ST6
ST7
sessionScore > limit
Yes
Flag the user
No
ST8
User total score > limit
Yes
No
ST4
Stop

Fig · 38

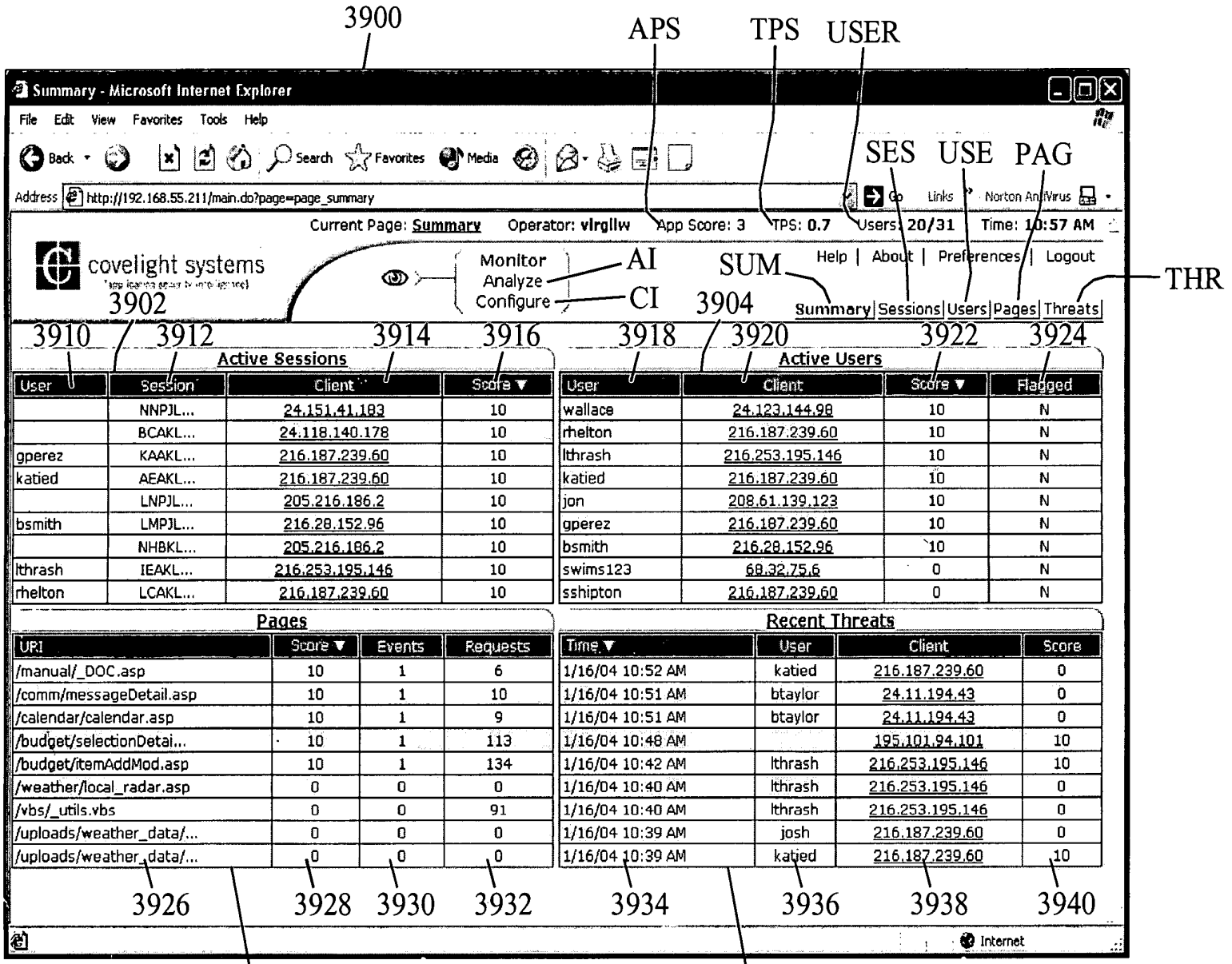

FIG. 39

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

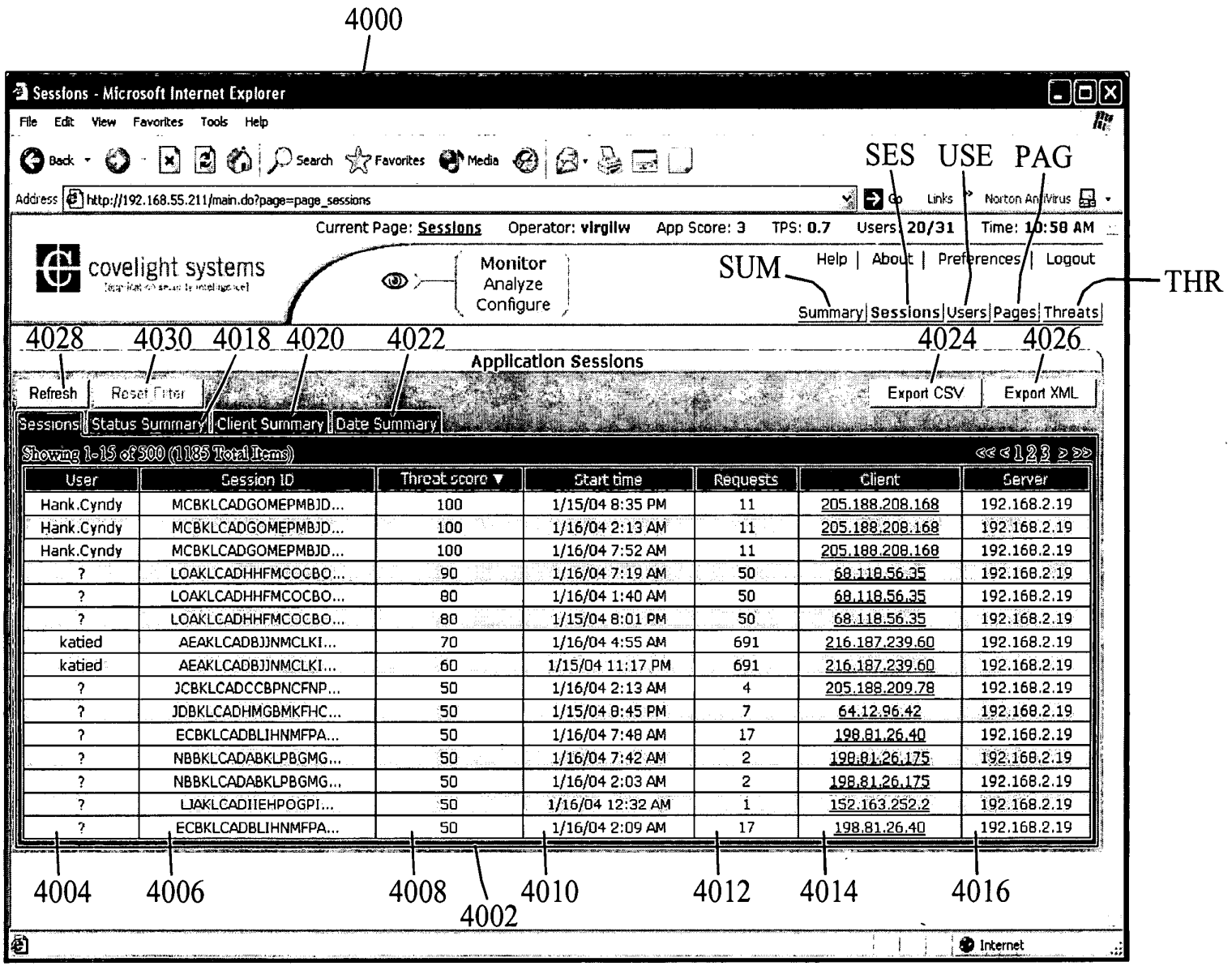

FIG. 40A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

4032

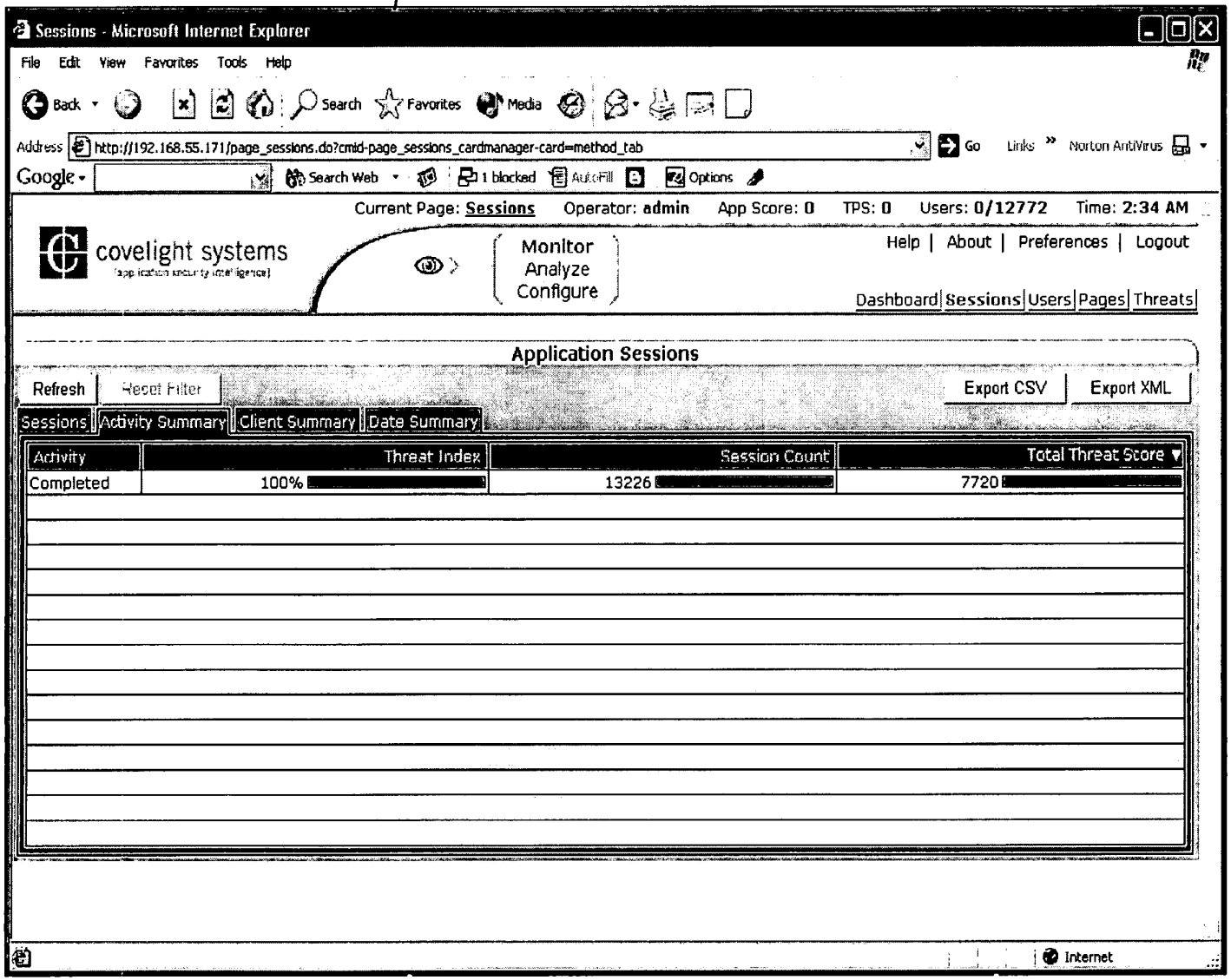

FIG. 40B

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

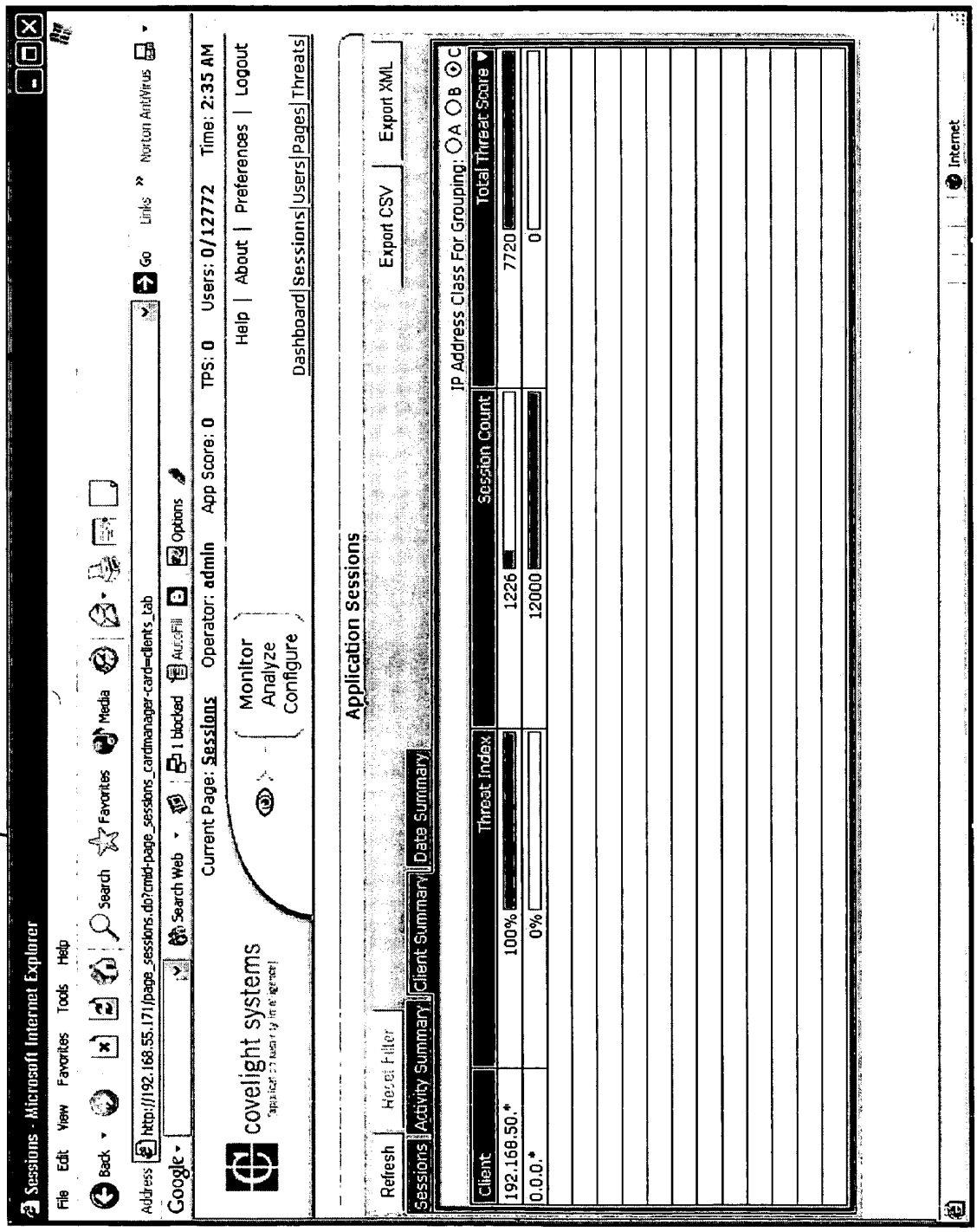
4034
Sessions - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.171/page_sessions.do?cmid=page_sessions_cardmanager-card=clients_tab
Google Search Web 1 blocked AutoFill Options
Norton AntiVirus
Current Page: Sessions Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:35 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard Sessions Users Pages Threats
Application Sessions
Refresh Header Filter
Export CSV Export XML
Sessions Activity Summary Client Summary Data Summary
IP Address Class For Grouping: A B C
Client
Threat Index
Session Count
Total Threat Score
192.168.50.*
100%
1226
7720
0.0.0.*
0%
12000
0
Internet

FIG. 40C

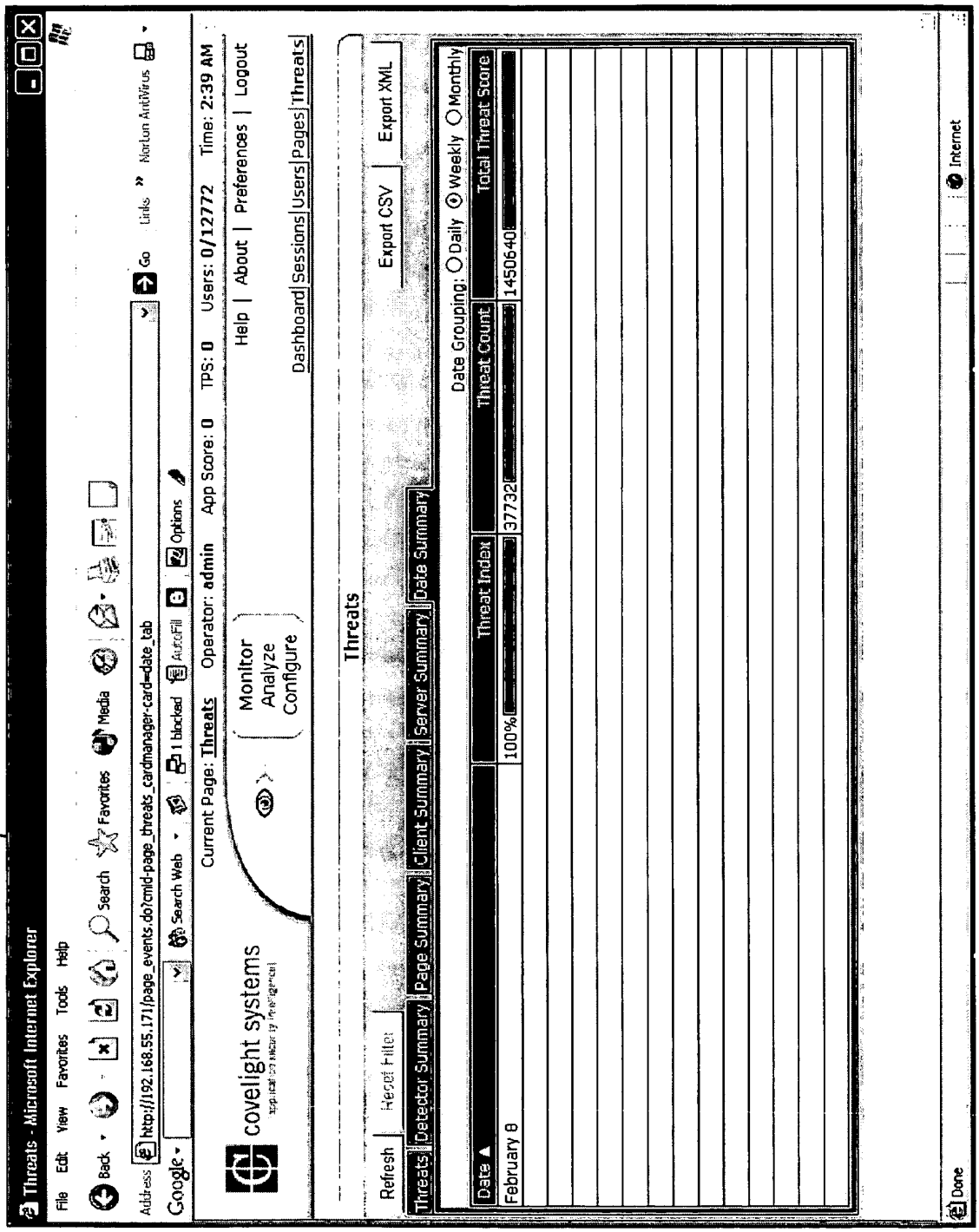
4036
Threats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.171/page_events.do?cmd-page_threats_cardmanager-card=date_tab
Google Search Web 1 blocked AutoFill Options
Go Links Norton AntiVirus
Current Page: Threats Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:39 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard Sessions Users Pages Threats
Threats
Refresh Reset Filter
Export CSV Export XML
Threats Detector Summary Page Summary Client Summary Server Summary Date Summary
Date Grouping: Daily Weekly Monthly
Date
Threat Index
Threat Count
Total Threat Score
February 8
100%
37732
1450640
Done
Internet

FIG. 40D

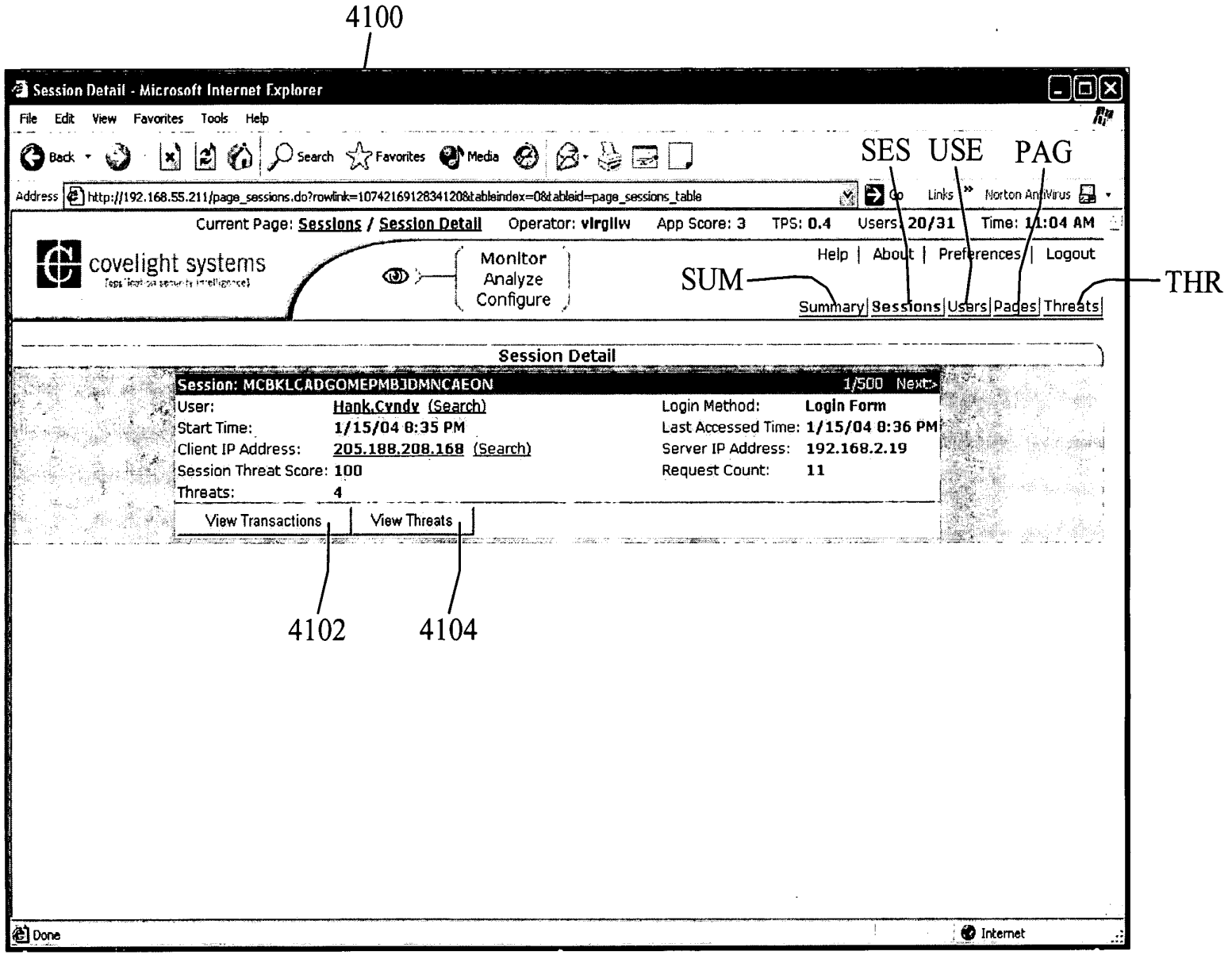

FIG. 41

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

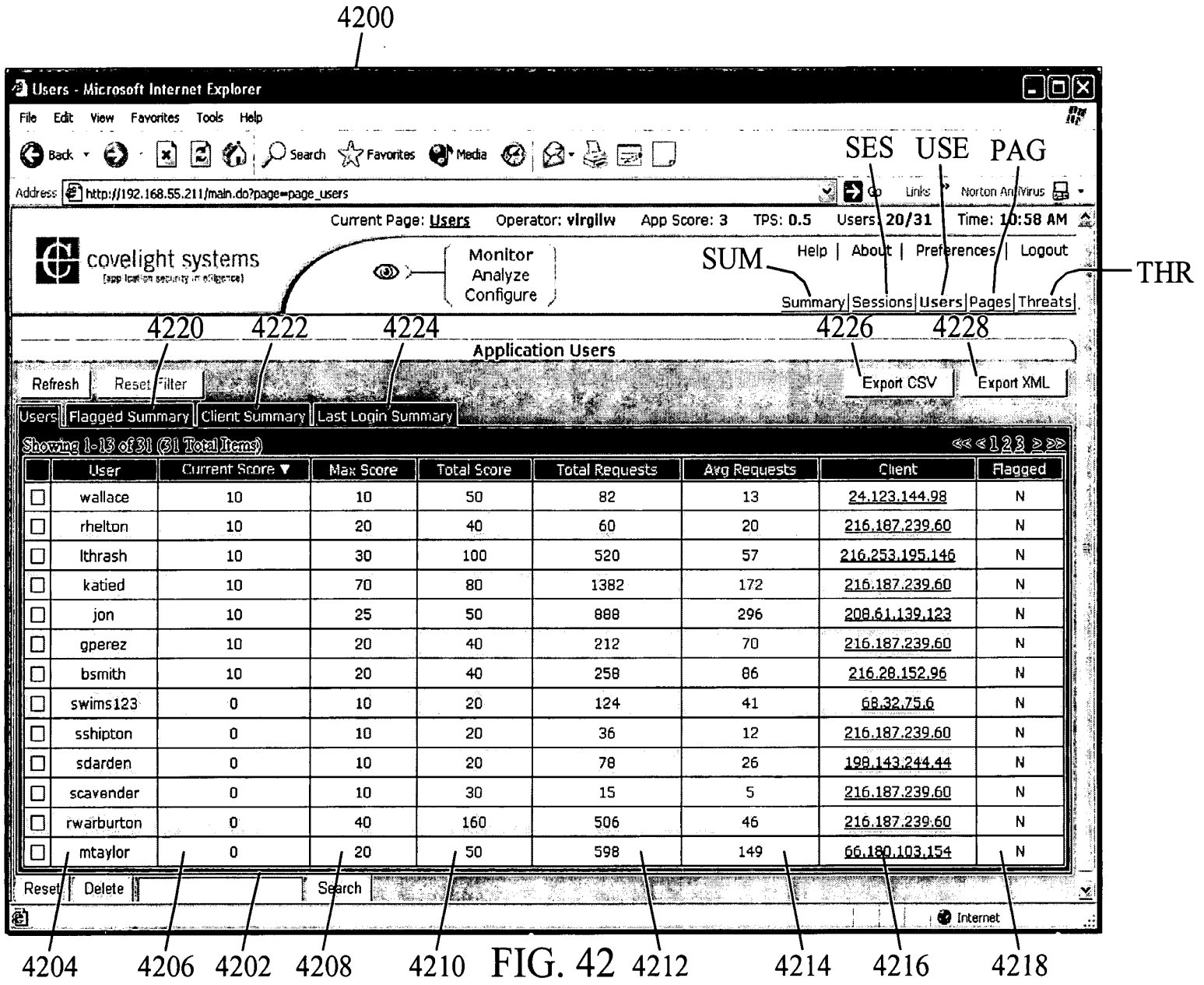

FIG. 42

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

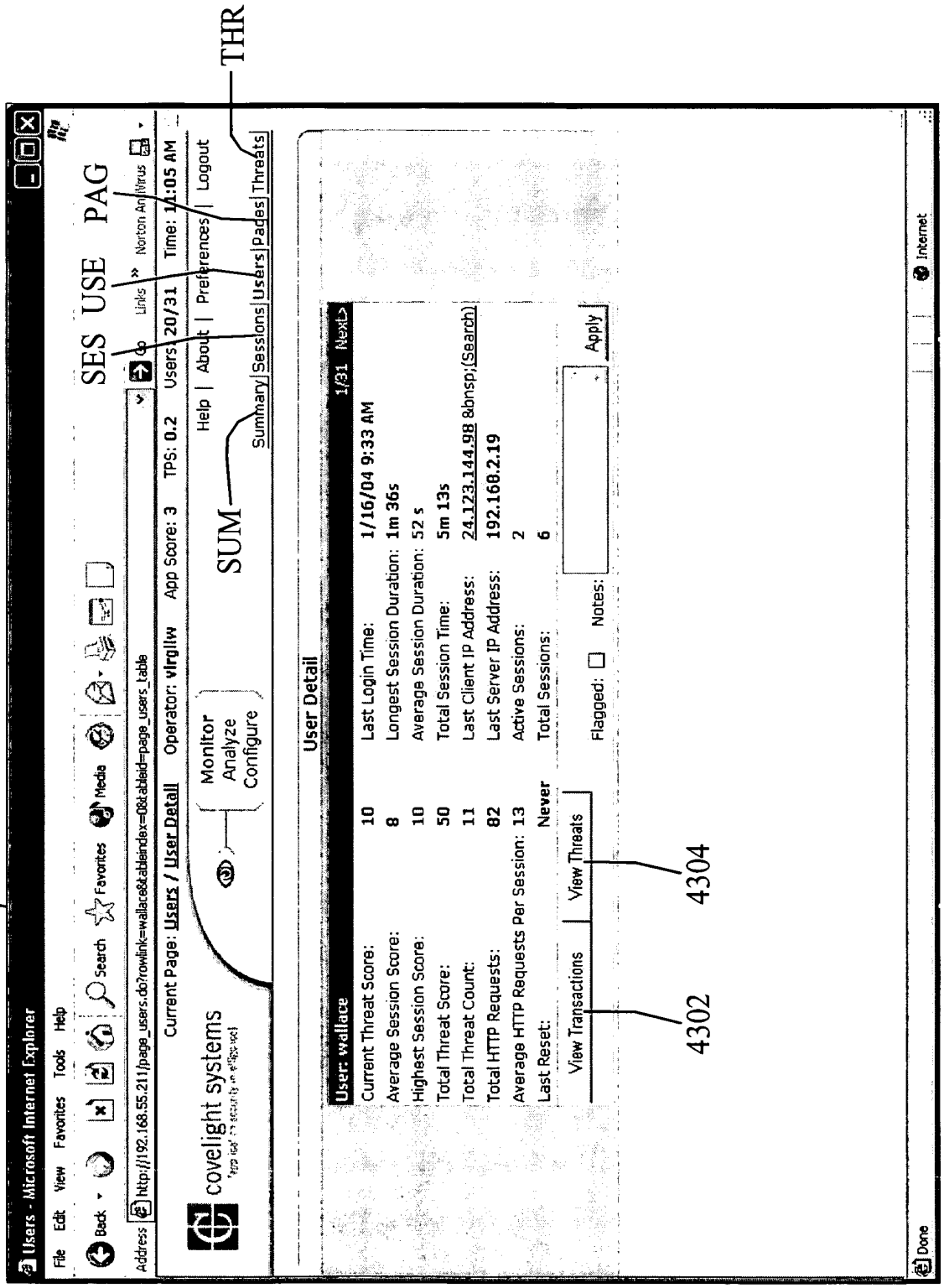
4300
THR
SES USE PAG
SUM
4302
4304
Users - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_users.do?rowlink=wallace&tabIndex=0&tabId=page_users_table
Norton AntiVirus
Links
Current Page: Users / User Detail
Operator: virgilw
App Score: 3
TPS: 0.2
Users: 20/31
Time: 14:05 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Summary Sessions Users Pades Threats
User Detail
User: wallace
1/31 Next>
Current Threat Score: 10
Average Session Score: 8
Highest Session Score: 10
Total Threat Score: 50
Total Threat Count: 11
Total HTTP Requests: 82
Average HTTP Requests Per Session: 13
Last Reset: Never
Last Login Time: 1/16/04 9:33 AM
Longest Session Duration: 1m 36s
Average Session Duration: 52 s
Total Session Time: 5m 13s
Last Client IP Address: 24.123.144.98 &bnsp;(Search)
Last Server IP Address: 192.168.2.19
Active Sessions: 2
Total Sessions: 6
View Transactions
View Threats
Flagged:
Notes:
Apply
Done
Internet

FIG. 43

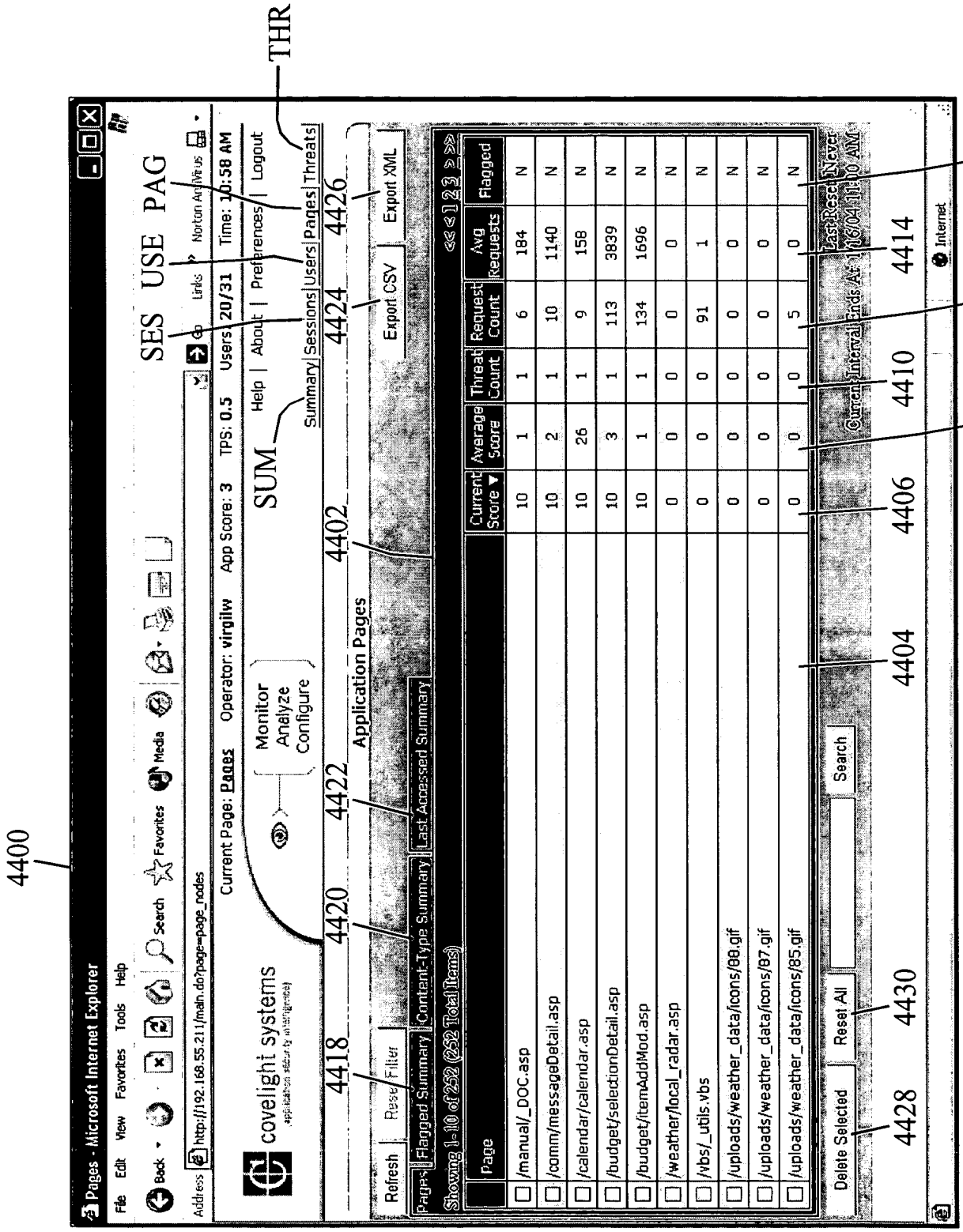
4400
THR
SES USE PAG
Pages - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?page=page_nodes
Links Norton AntiVirus
Current Page: Pages Operator: virgilw App Score: 3 TPS: 0.5 Users: 20/31 Time: 10:58 AM
covelight systems
Monitor
Analyze
Configure
SUM
Help | About | Preferences | Logout
Summary | Sessions | Users | Pages | Threats
4418 4420 4422 4402 4424 4426
Application Pages
Export CSV Export XML
Refresh Reset Filter
Pages | Flagged Summary | Content-Type Summary | Last Accessed Summary
Showing 1 - 10 of 252 (252 Total Items)
<< < 1 2 3 > >>
Page | Current Score | Average Score | Threat Count | Request Count | Avg Requests | Flagged
/manual/_DOC.asp 10 1 1 6 184 N
/comm/messageDetail.asp 10 2 1 10 1140 N
/calendar/calendar.asp 10 26 1 9 158 N
/budget/selectionDetail.asp 10 3 1 113 3839 N
/budget/itemAddMod.asp 10 1 1 134 1696 N
/weather/local_radar.asp 0 0 0 0 0 N
/vbs/_utils.vbs 0 0 0 91 1 N
/uploads/weather_data/icons/88.gif 0 0 0 0 0 N
/uploads/weather_data/icons/87.gif 0 0 0 0 0 N
/uploads/weather_data/icons/85.gif 0 0 0 5 0 N
Delete Selected Reset All Search
Current Interval Ends At: 1/6/04 11:10 AM
Last Reset: Never
Internet
4428 4430 4404 4406 4408 4410 4412 4414 4416

FIG. 44

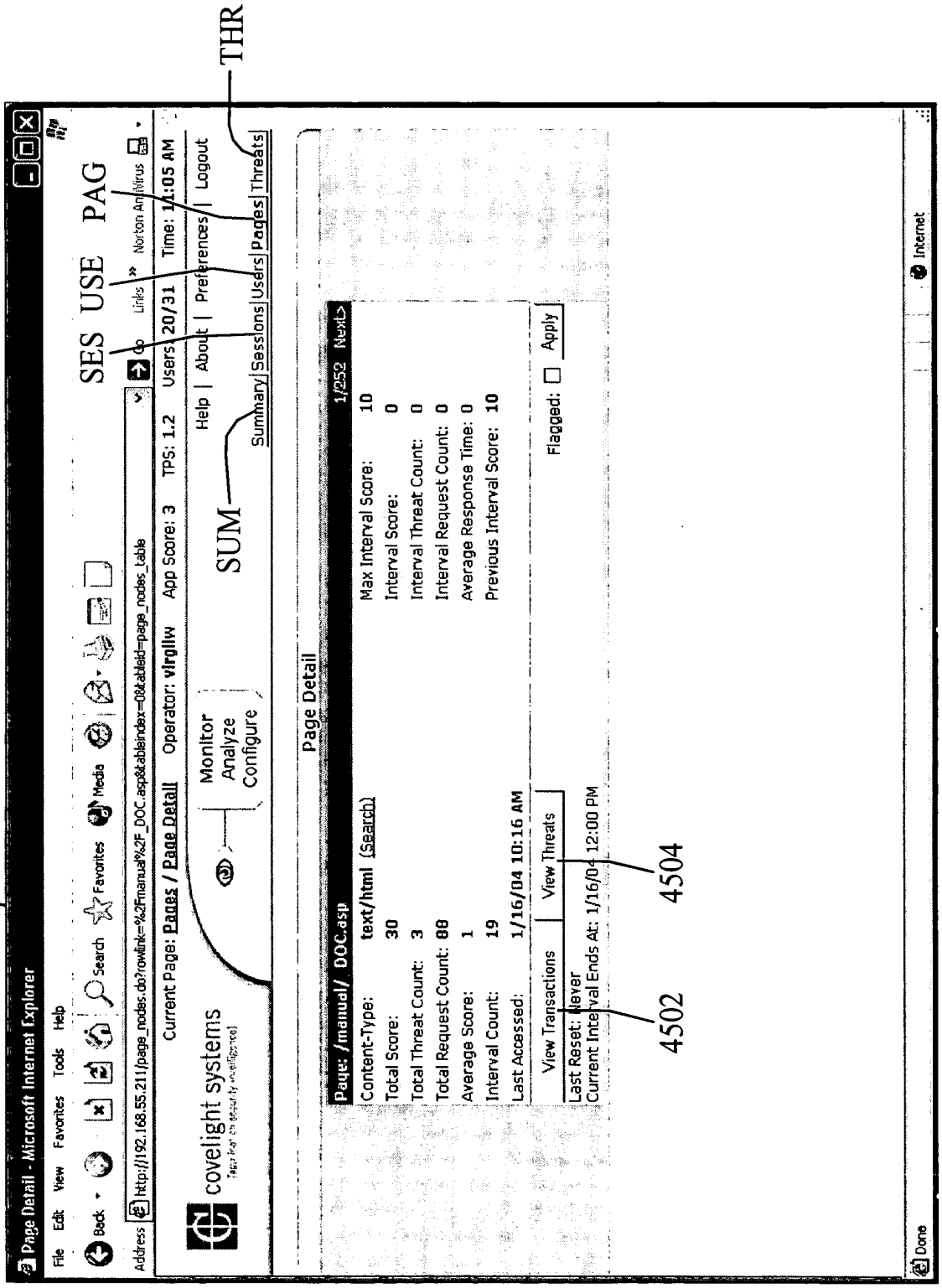
4500
Page Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_nodes.do?rowlink=%2Fmanual%2F_DOC.asp&tableindex=0&tableId=page_nodes_table
Links Norton AntiVirus
Current Page: Pages / Page Detail Operator: virgilw App Score: 3 TPS: 1.2 Users: 20/31 Time: 14:05 AM
covelight systems
Monitor
Analyze
Configure
SUM
Help | About | Preferences | Logout
Summary Sessions Users Pages Threats
SES USE PAG
THR
Page Detail
Page: /manual/_DOC.asp
1/252 Next>
Content-Type: text/html (Search)
Total Score: 30
Total Threat Count: 3
Total Request Count: 80
Average Score: 1
Interval Count: 19
Last Accessed: 1/16/04 10:16 AM
Max Interval Score: 10
Interval Score: 0
Interval Threat Count: 0
Interval Request Count: 0
Average Response Time: 0
Previous Interval Score: 10
View Transactions
View Threats
Flagged: Apply
Last Reset: Never
Current Interval Ends At: 1/16/04 12:00 PM
4502
4504
Done
Internet

FIG. 45

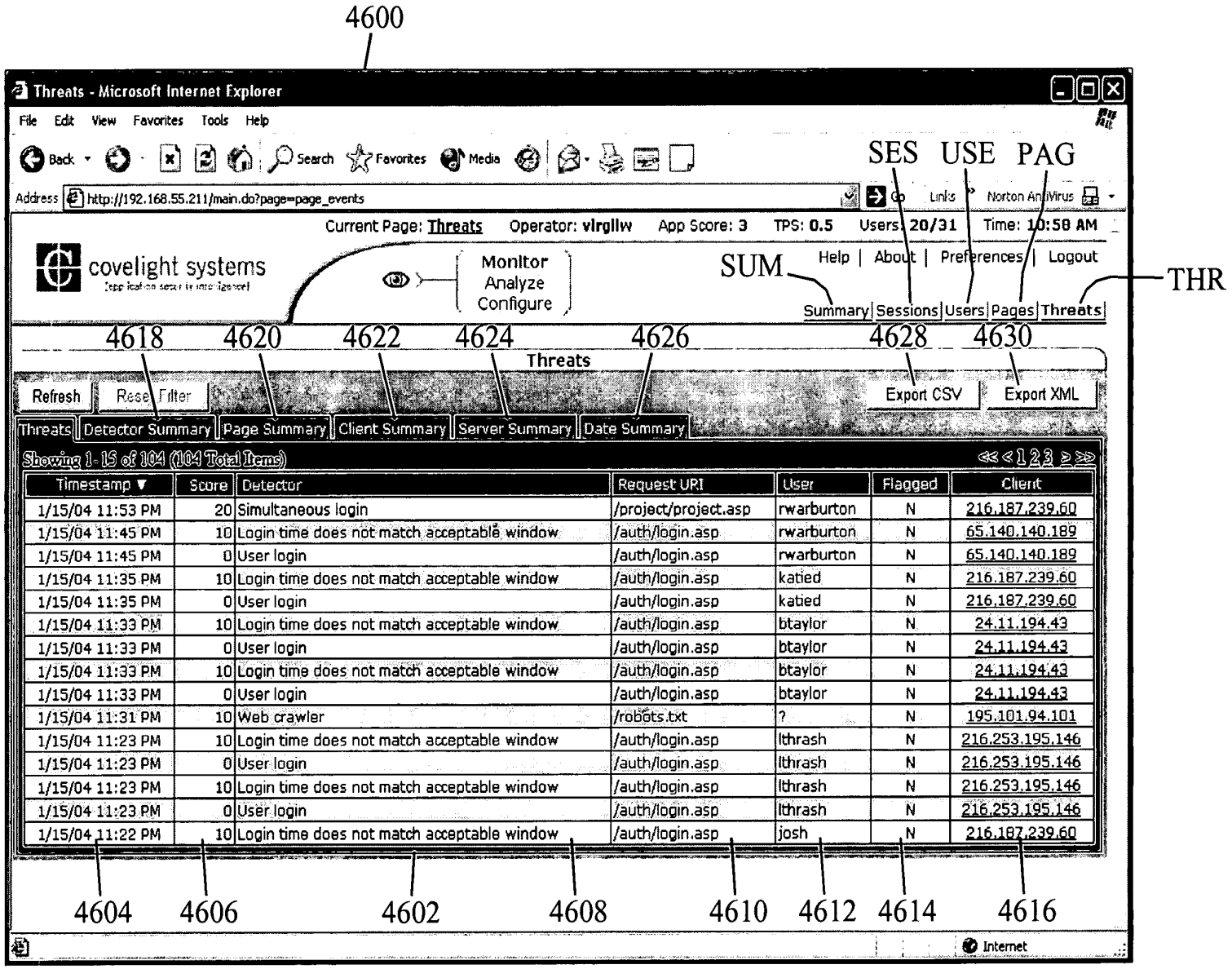

FIG. 46A

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

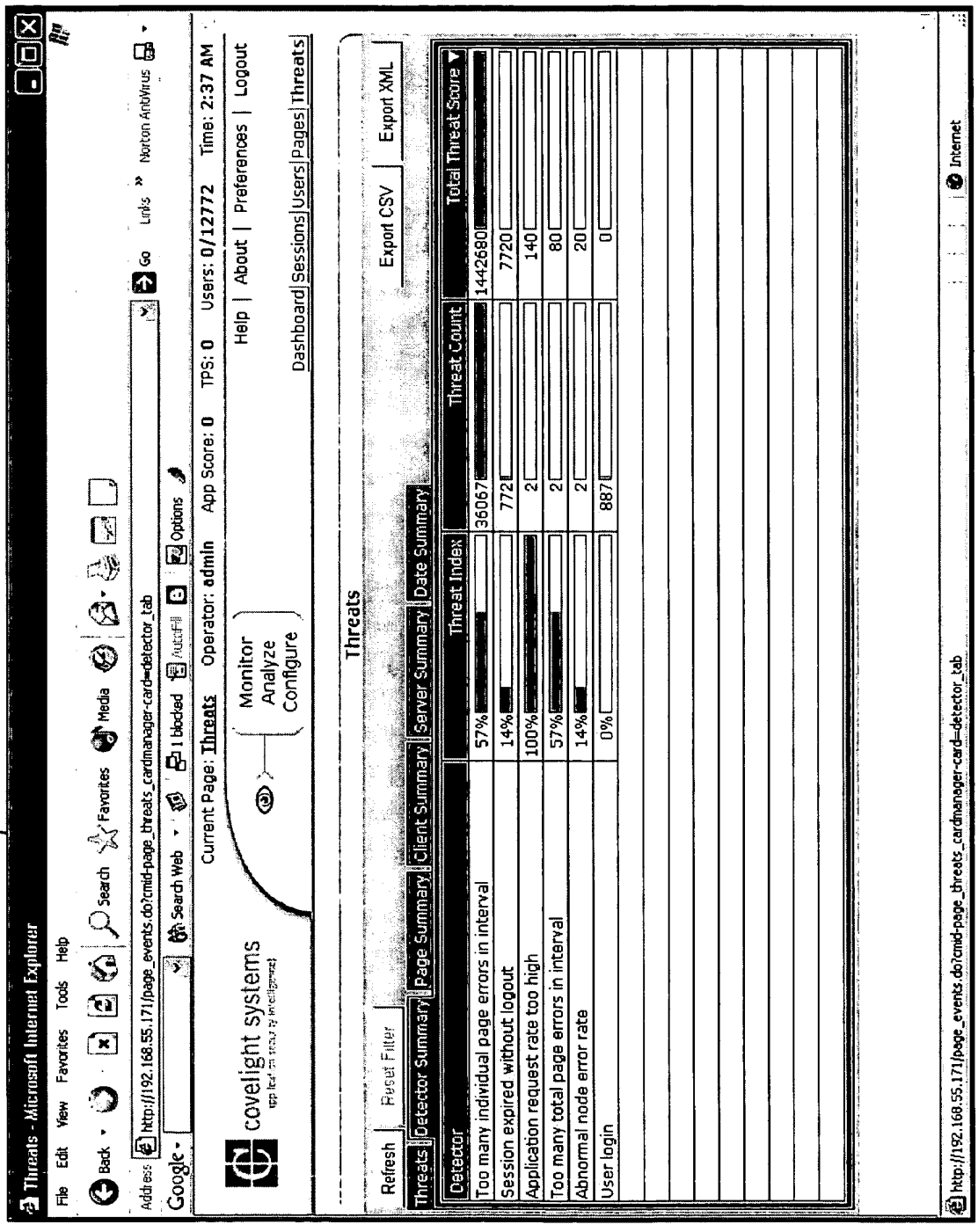
4632
Threats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.171/page_events.do?cmid=page_threats_cardmanager-card=detector_tab
Google Search Web 1 blocked AutoFill Options
Go Links Norton AntiVirus
Current Page: Threats Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:37 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard Sessions Users Pages Threats
Threats
Refresh Reset Filter
Export CSV Export XML
Threats Detector Summary Page Summary Client Summary Server Summary Date Summary
Detector
Threat Index
Threat Count
Total Threat Score
Too many individual page errors in interval 57% 36067 1442680
Session expired without logout 14% 772 7720
Application request rate too high 100% 2 140
Too many total page errors in interval 57% 2 80
Abnormal node error rate 14% 2 20
User login 0% 887 0
http://192.168.55.171/page_events.do?cmid=page_threats_cardmanager-card=detector_tab
Internet

FIG. 46B

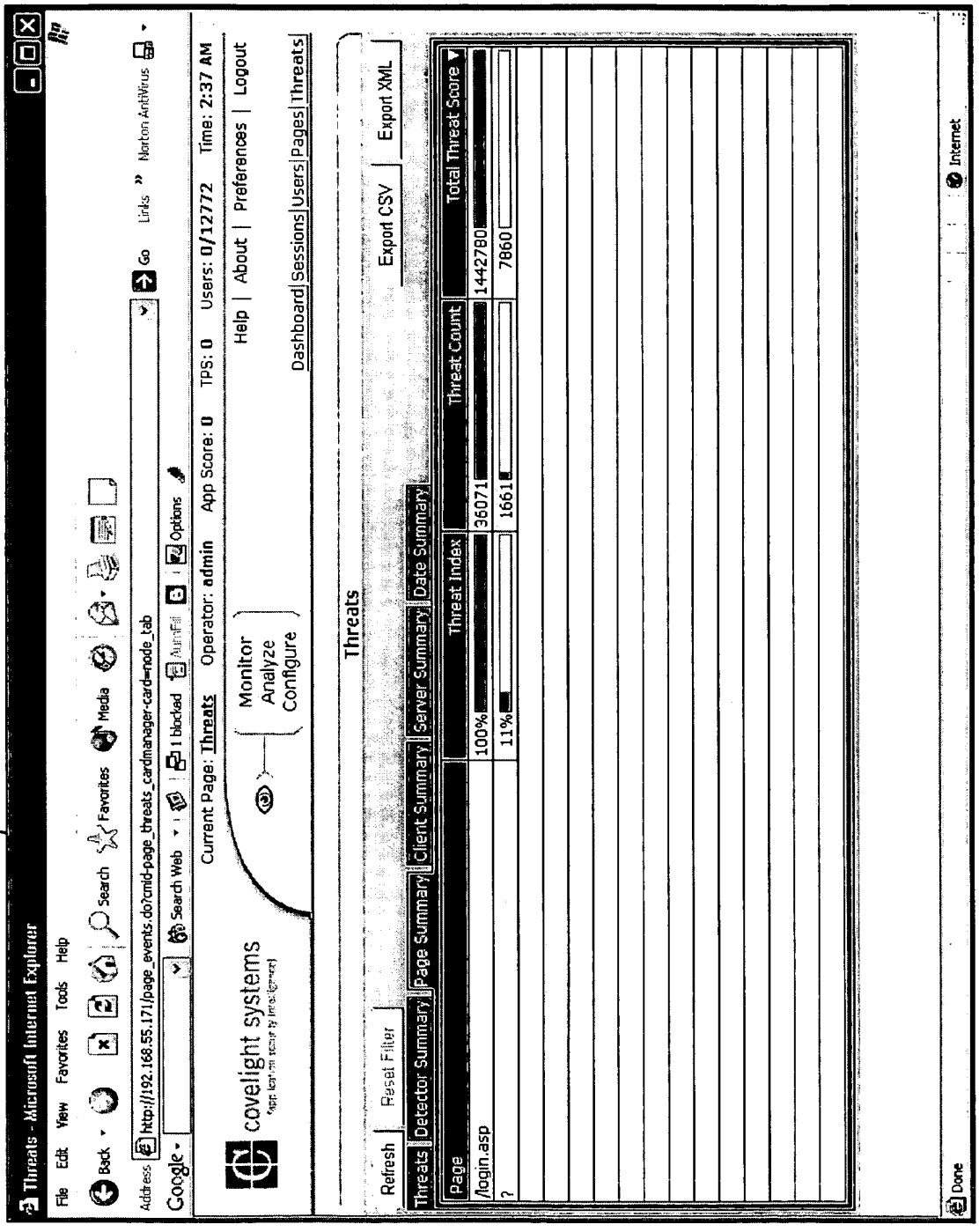
4634
Threats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.171/page_events.do?cmid=page_threats_cardmanager-card=node_tab
Google Search Web 1 blocked AutoFill Options
Go Links Norton AntiVirus
Current Page: Threats Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:37 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard Sessions Users Pages Threats
Threats
Refresh Reset Filter
Export CSV Export XML
Threats Detector Summary Page Summary Client Summary Server Summary Date Summary
Page
Threat Index
Threat Count
Total Threat Score
/login.asp
100%
36071
1442780
?
11%
1661
7860
Done
Internet

FIG. 46C

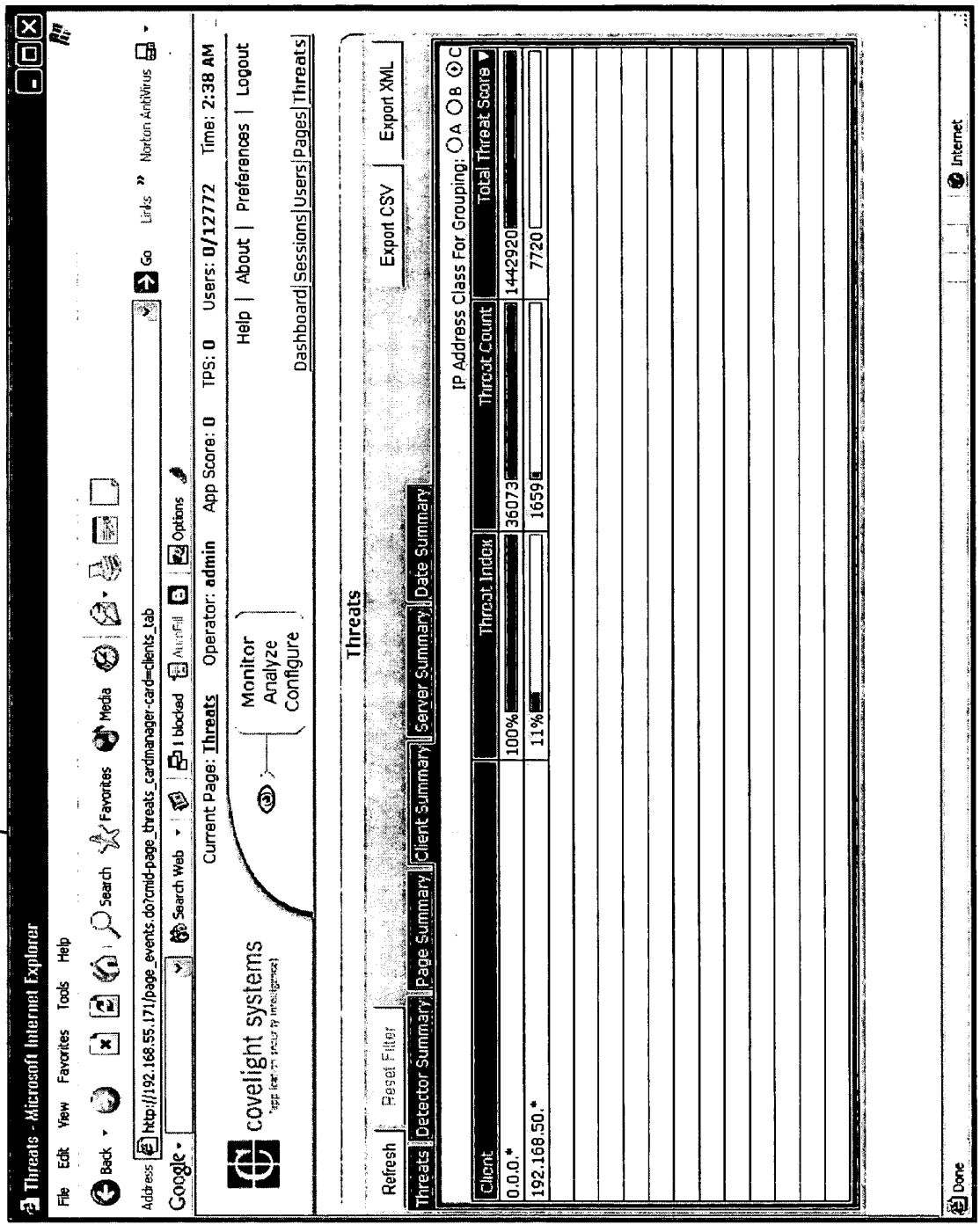
4636
Threats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.171/page_events.do?cmid=page_threats_cardmanager-card=clients_tab
Google Search Web 1 blocked AutoFill Options
Go Links Norton AntiVirus
Current Page: Threats Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:38 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard Sessions Users Pages Threats
Threats
Refresh Reset Filter
Export CSV Export XML
Threats Detector Summary Page Summary Client Summary Server Summary Date Summary
IP Address Class For Grouping: A B C
Client
Throat Index
Throat Count
Total Threat Score
0.0.0.*
100%
36073
1442920
192.168.50.*
11%
1659
7720
Done
Internet

FIG. 46D

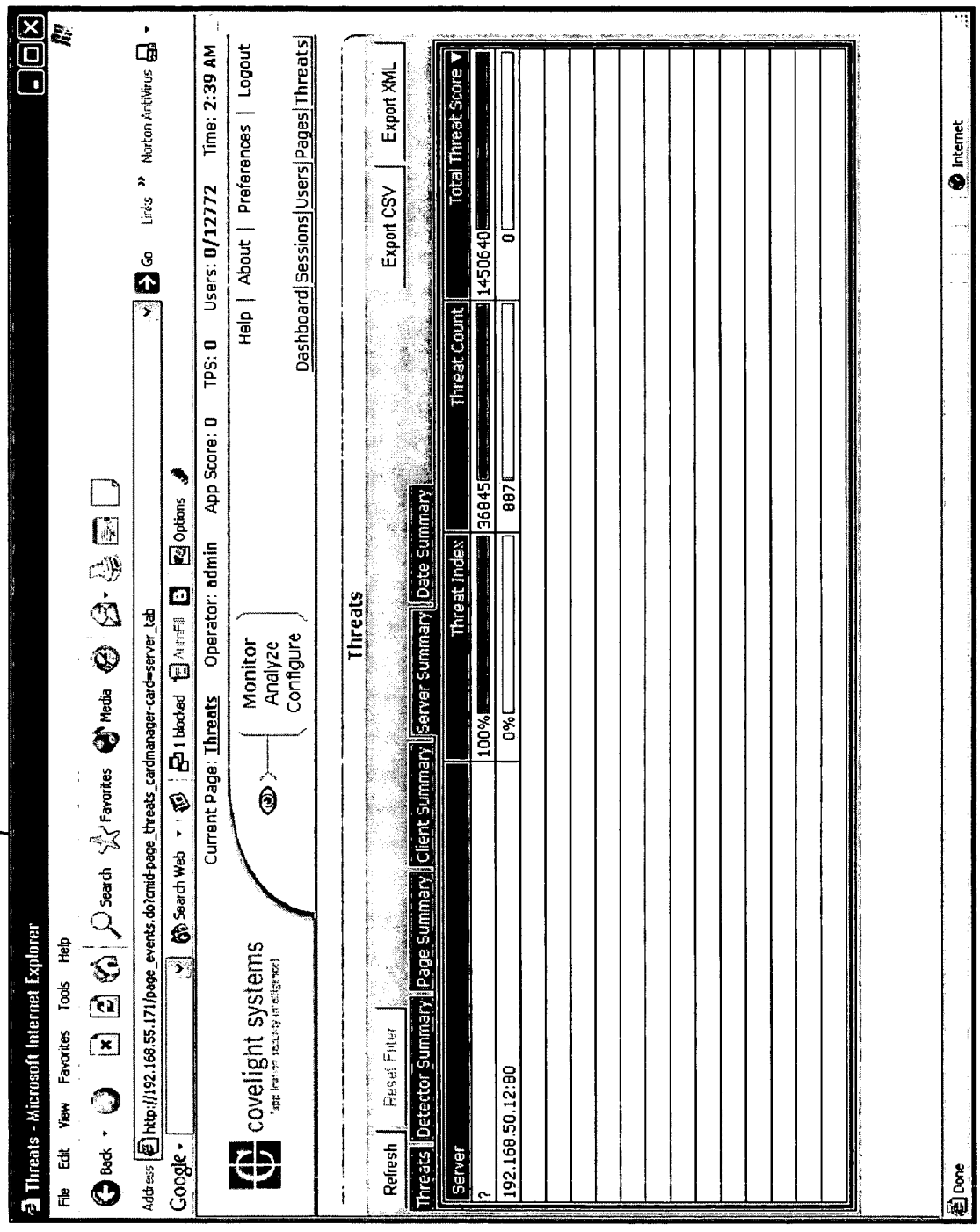
4638
Threats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.171/page_events.do?cmid=page_threats_cardmanager-card=server_tab
Google Search Web 1 blocked AutoFill Options
Go Links Norton AntiVirus
Current Page: Threats Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:39 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard Sessions Users Pages Threats
Threats
Refresh Reset Filter
Export CSV Export XML
Threats Detector Summary Page Summary Client Summary Server Summary Date Summary
Server
Threat Index
Threat Count
Total Threat Score
? 100% 36845 1450640
192.168.50.12:80 0% 887 0
Done
Internet

FIG. 46E

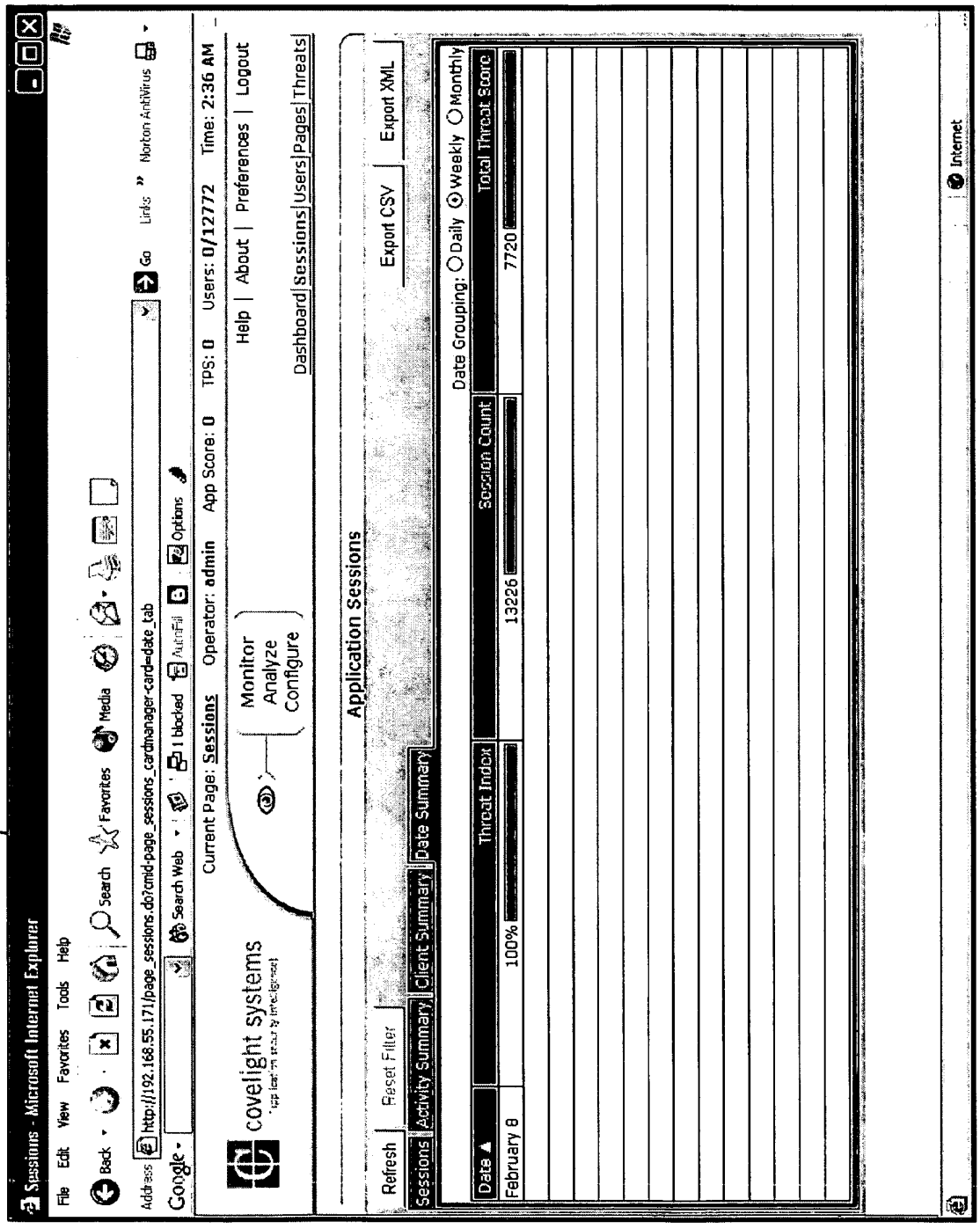
4640
Sessions - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.171/page_sessions.do?cmid=page_sessions_cardmanager-card=date_tab
Google Search Web 1 blocked AutoFill Options
Go Links Norton AntiVirus
Current Page: Sessions Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:36 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Dashboard|Sessions|Users|Pages|Threats
Application Sessions
Refresh Reset Filter
Export CSV Export XML
Sessions Activity Summary Client Summary Date Summary
Date Grouping: Daily Weekly Monthly
Date
Threat Index
Session Count
Total Threat Score
February 8
100%
13226
7720
Internet

FIG. 46F

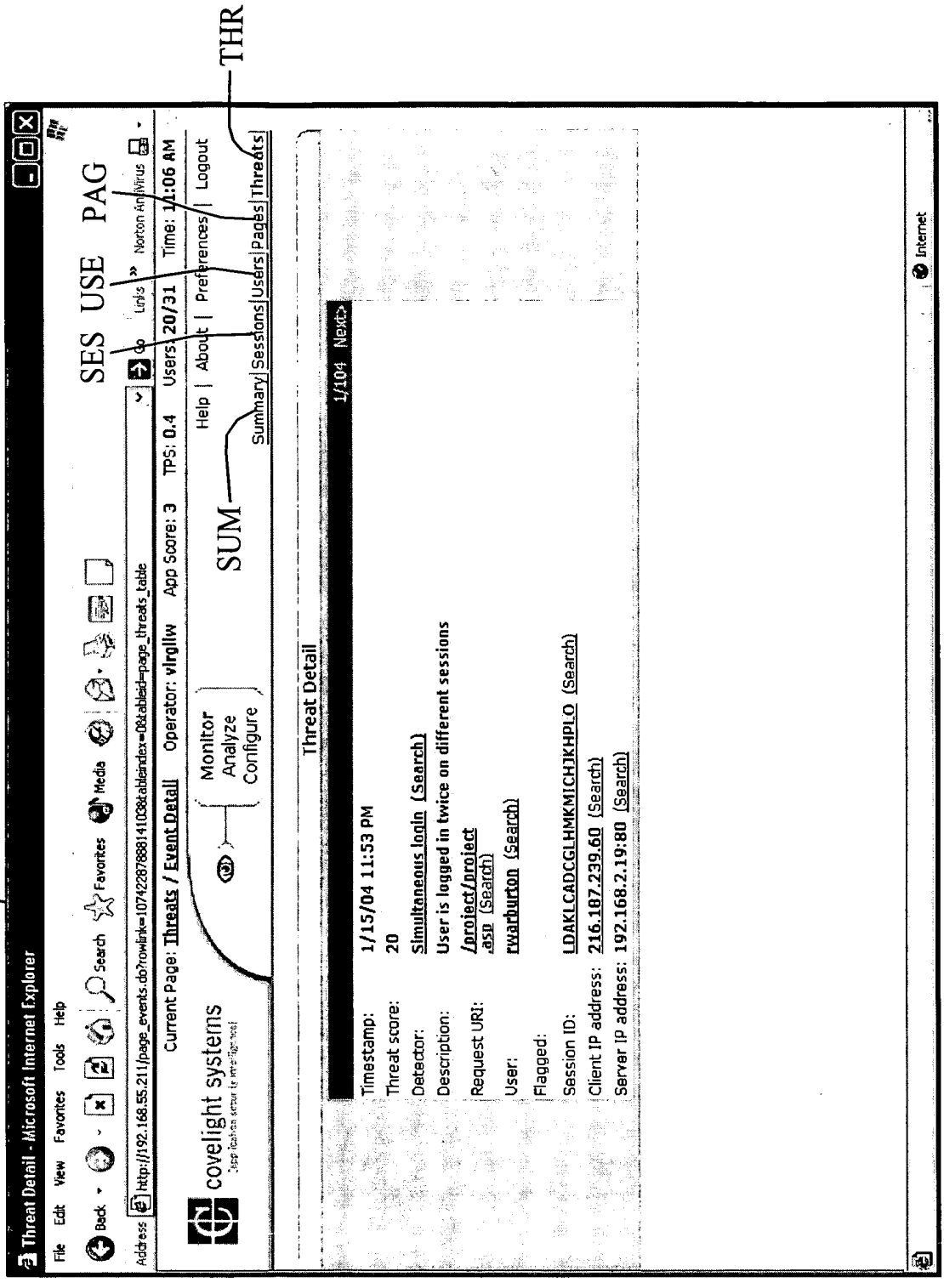
4700
THR
Threat Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
SES USE PAG
Address http://192.168.55.211/page_events.do?rowlink=1074228788814103&tabledindex=0&tableid=page_threats_table
Links Norton AntiVirus
Current Page: Threats / Event Detail Operator: virgilw App Score: 3 TPS: 0.4 Users: 20/31 Time: 1:06 AM
covelight systems
Monitor
Analyze
Configure
SUM
Help | About | Preferences | Logout
Summary Sessions Users Pages Threats
Threat Detail
1/104 Next>
Timestamp: 1/15/04 11:53 PM
Threat score: 20
Detector: Simultaneous login (Search)
Description: User is logged in twice on different sessions
Request URI: /project/project.asp (Search)
User: rwarburton (Search)
Flagged:
Session ID: LDAKLCADCGLHMKMICHJKHPLO (Search)
Client IP address: 216.187.239.60 (Search)
Server IP address: 192.168.2.19:80 (Search)
Internet

FIG. 47

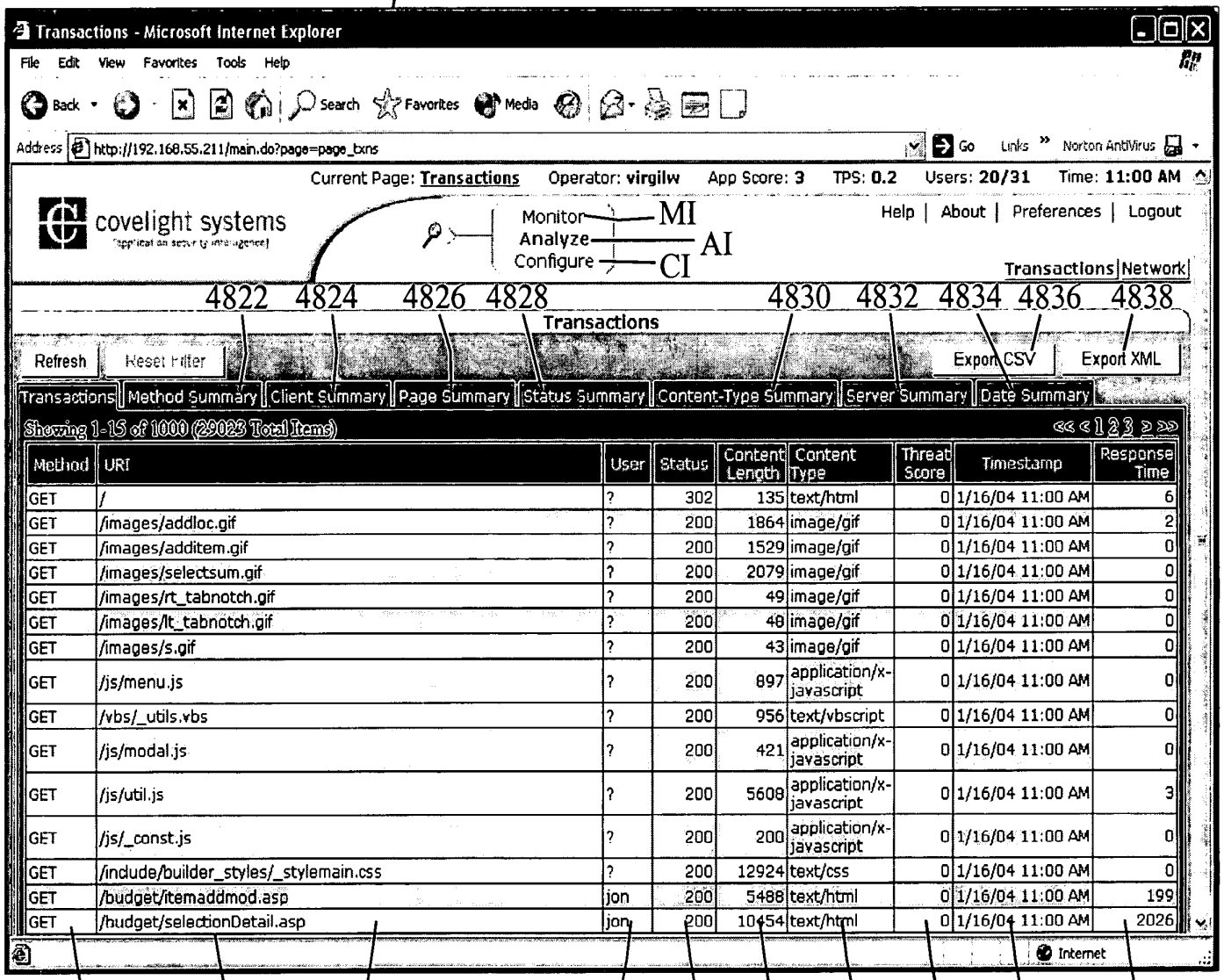
4800
Transactions - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?page=page_txns
Go Links Norton AntiVirus
Current Page: Transactions Operator: virgilw App Score: 3 TPS: 0.2 Users: 20/31 Time: 11:00 AM
covelight systems
Monitor MI
Analyze AI
Configure CI
Help | About | Preferences | Logout
Transactions | Network
4822 4824 4826 4828 4830 4832 4834 4836 4838
Transactions
Refresh Reset Filter Export CSV Export XML
Transactions | Method Summary | Client Summary | Page Summary | Status Summary | Content-Type Summary | Server Summary | Date Summary
Showing 1-15 of 1000 (29023 Total Items)
« < 1 2 3 > »
Method | URI | User | Status | Content Length | Content Type | Threat Score | Timestamp | Response Time
GET | / | ? | 302 | 135 | text/html | 0 | 1/16/04 11:00 AM | 6
GET | /images/addloc.gif | ? | 200 | 1864 | image/gif | 0 | 1/16/04 11:00 AM | 2
GET | /images/additem.gif | ? | 200 | 1529 | image/gif | 0 | 1/16/04 11:00 AM | 0
GET | /images/selectsum.gif | ? | 200 | 2079 | image/gif | 0 | 1/16/04 11:00 AM | 0
GET | /images/rt_tabnotch.gif | ? | 200 | 49 | image/gif | 0 | 1/16/04 11:00 AM | 0
GET | /images/lt_tabnotch.gif | ? | 200 | 48 | image/gif | 0 | 1/16/04 11:00 AM | 0
GET | /images/s.gif | ? | 200 | 43 | image/gif | 0 | 1/16/04 11:00 AM | 0
GET | /js/menu.js | ? | 200 | 897 | application/x-javascript | 0 | 1/16/04 11:00 AM | 0
GET | /vbs/_utils.vbs | ? | 200 | 956 | text/vbscript | 0 | 1/16/04 11:00 AM | 0
GET | /js/modal.js | ? | 200 | 421 | application/x-javascript | 0 | 1/16/04 11:00 AM | 0
GET | /js/util.js | ? | 200 | 5608 | application/x-javascript | 0 | 1/16/04 11:00 AM | 3
GET | /js/_const.js | ? | 200 | 200 | application/x-javascript | 0 | 1/16/04 11:00 AM | 0
GET | /include/builder_styles/_stylemain.css | ? | 200 | 12924 | text/css | 0 | 1/16/04 11:00 AM | 0
GET | /budget/itemaddmod.asp | jon | 200 | 5488 | text/html | 0 | 1/16/04 11:00 AM | 199
GET | /budget/selectionDetail.asp | jon | 200 | 10454 | text/html | 0 | 1/16/04 11:00 AM | 2026
Internet
4804 4802 4806 4808 4810 4812 4814 4816 4818 4820

FIG. 48

4900

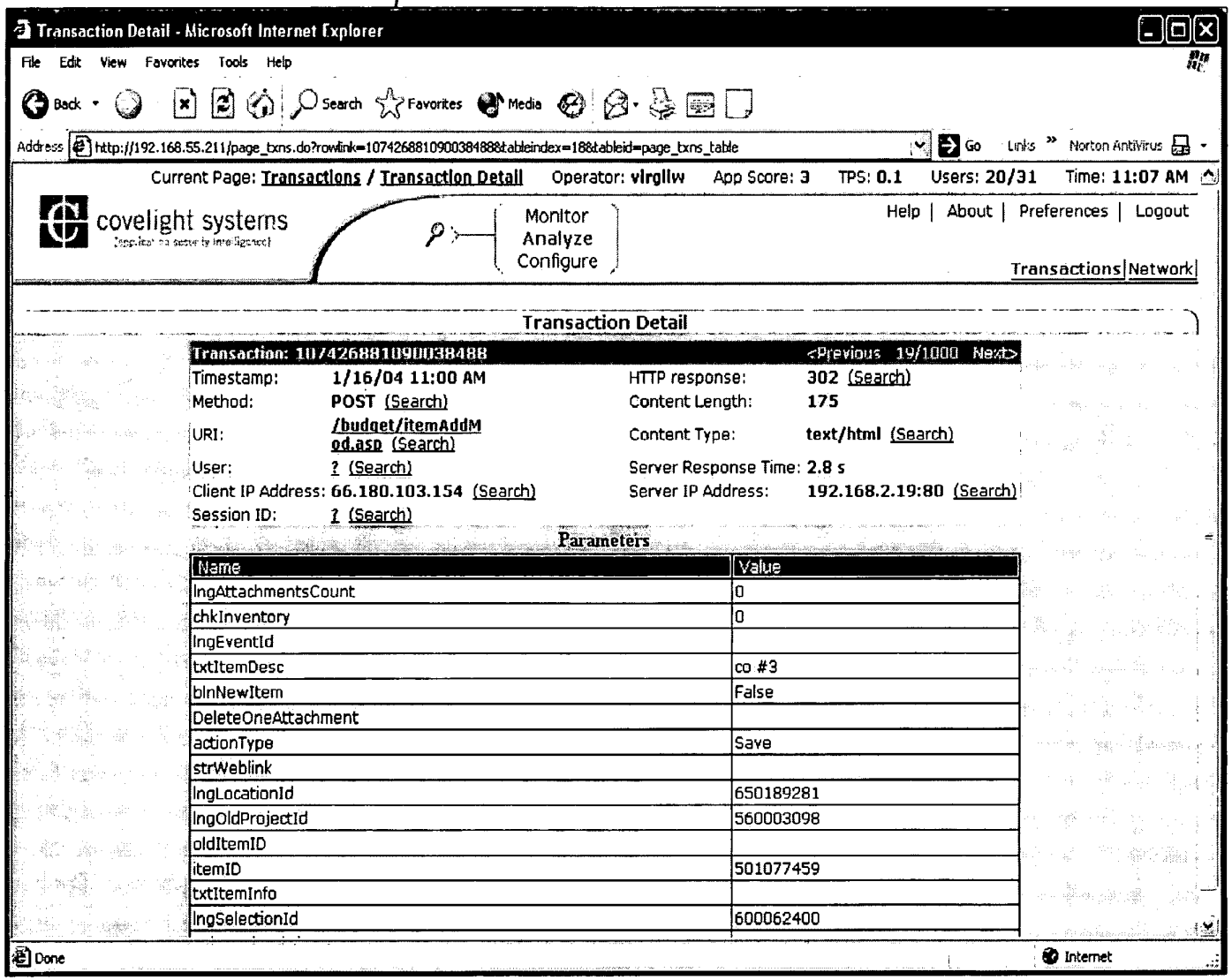

FIG. 49

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

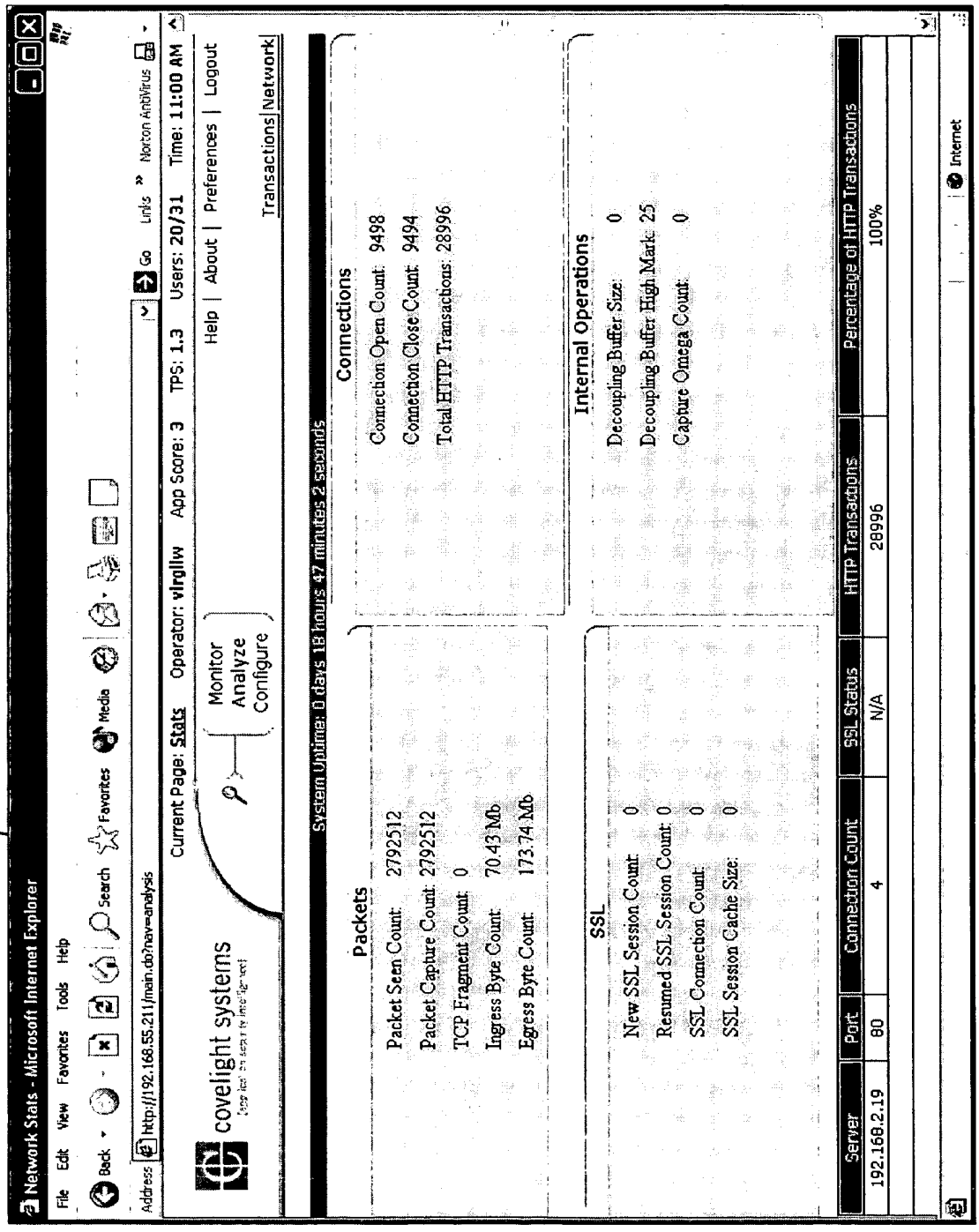
5000
Network Stats - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?nav=analysis
Go Links Norton AntiVirus
Current Page: Stats Operator: virgilw App Score: 3 TPS: 1.3 Users: 20/31 Time: 11:00 AM
Help | About | Preferences | Logout
covelight systems
Monitor
Analyze
Configure
Transactions Network
System Uptime: 0 days 18 hours 47 minutes 2 seconds
Packets
Packet Seen Count: 2792512
Packet Capture Count: 2792512
TCP Fragment Count: 0
Ingress Byte Count: 70.43 Mb
Egress Byte Count: 173.74 Mb
Connections
Connection Open Count: 9498
Connection Close Count: 9494
Total HTTP Transactions: 28996
Internal Operations
Decoupling Buffer Size: 0
Decoupling Buffer High Mark: 25
Capture Omega Count: 0
SSL
New SSL Session Count: 0
Resumed SSL Session Count: 0
SSL Connection Count: 0
SSL Session Cache Size: 0
Server | Port | Connection Count | SSL Status | HTTP Transactions | Percentage of HTTP Transactions
192.168.2.19 | 80 | 4 | N/A | 28996 | 100%
Internet

FIG. 50

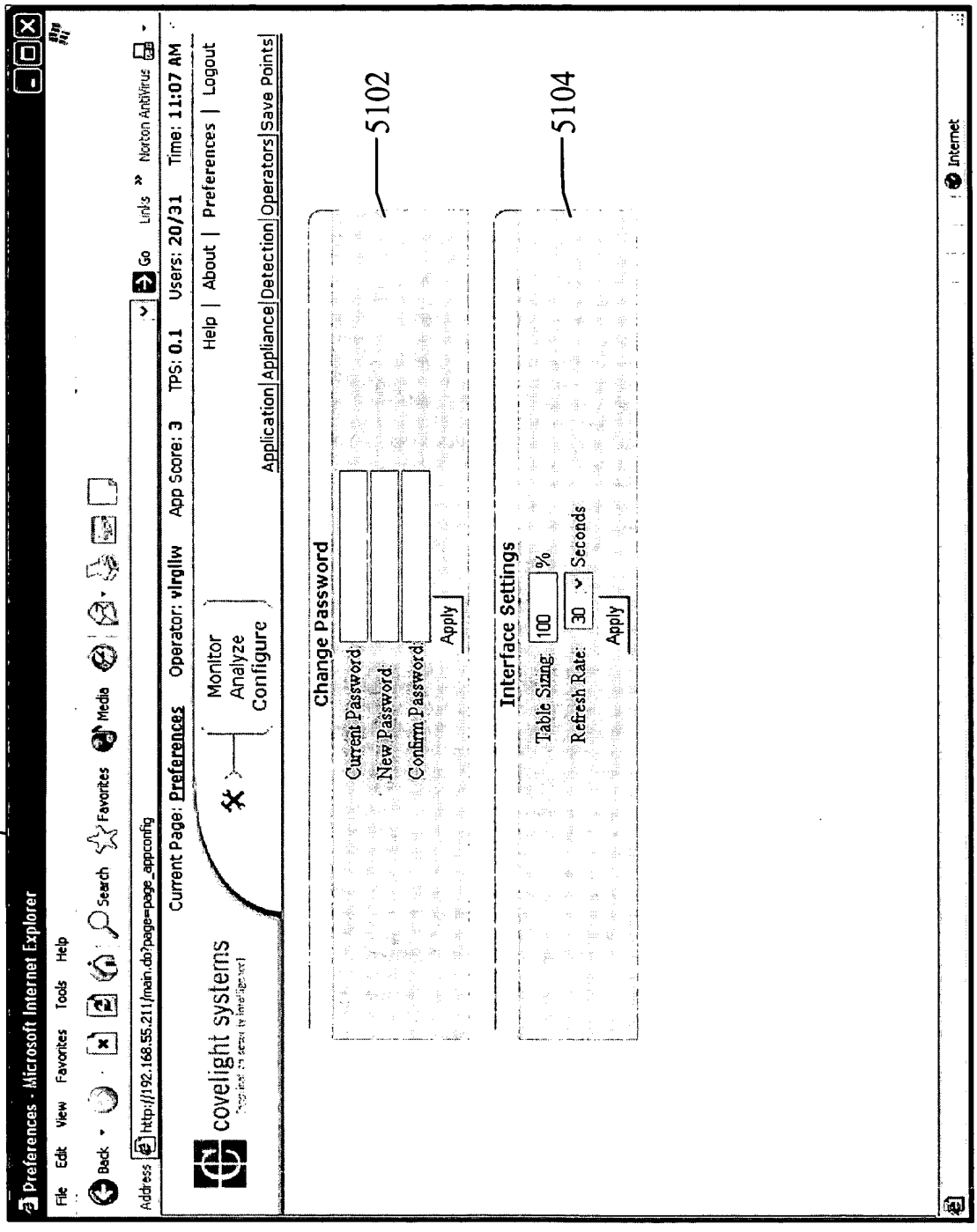
5100
Preferences - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?page=page_appconfig
Go Links Norton AntiVirus
Current Page: Preferences Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:07 AM
Help | About | Preferences | Logout
covelight systems
Monitor
Analyze
Configure
Application Appliance Detection Operators Save Points
Change Password
Current Password
New Password
Confirm Password
Apply
5102
Interface Settings
Table Size: 100 %
Refresh Rate: 30 Seconds
Apply
5104
Internet

FIG. 51

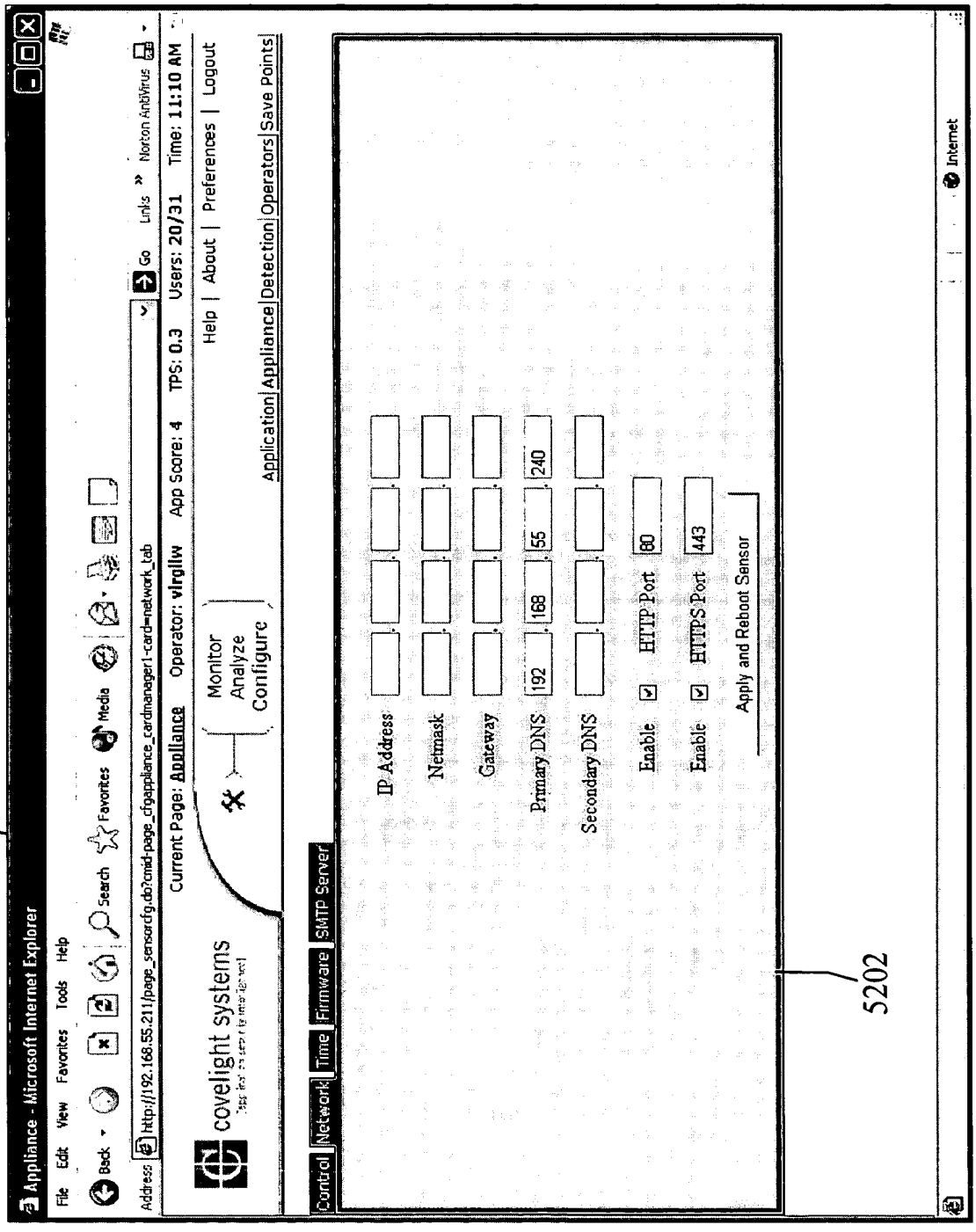
5200
Appliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_sensorcfg.do?cmd=page_cfgappliance_cardmanager1-card=network_tab
Go Links Norton AntiVirus
Current Page: Appliance Operator: virgilw App Score: 4 TPS: 0.3 Users: 20/31 Time: 11:10 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
Control Network Time Firmware SMTP Server
IP Address
Netmask
Gateway
Primary DNS 192 168 55 240
Secondary DNS
Enable HTTP Port 80
Enable HTTPS Port 443
Apply and Reboot Sensor
5202
Internet

FIG. 52

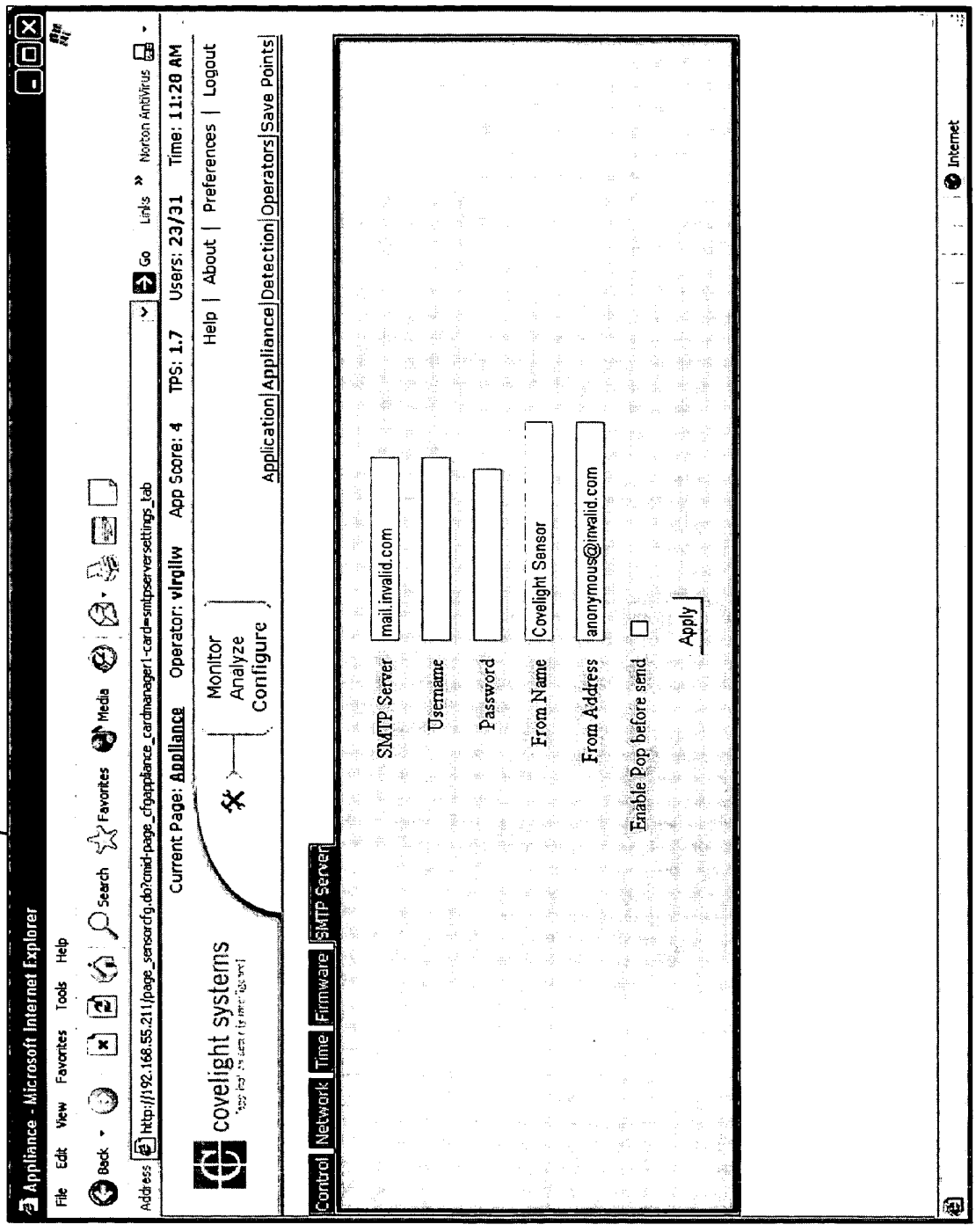
5300
Appliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_sensorcfg.do?cmid=page_cfgappliance_cardmanager1-card=smtpserversettings_tab
Go Links Norton AntiVirus
Current Page: Appliance Operator: virgilw App Score: 4 TPS: 1.7 Users: 23/31 Time: 11:20 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
Control Network Time Firmware SMTP Server
SMTP Server mail.invalid.com
Username
Password
From Name Covelight Sensor
From Address anonymous@invalid.com
Enable Pop before send
Apply
Internet

FIG. 53

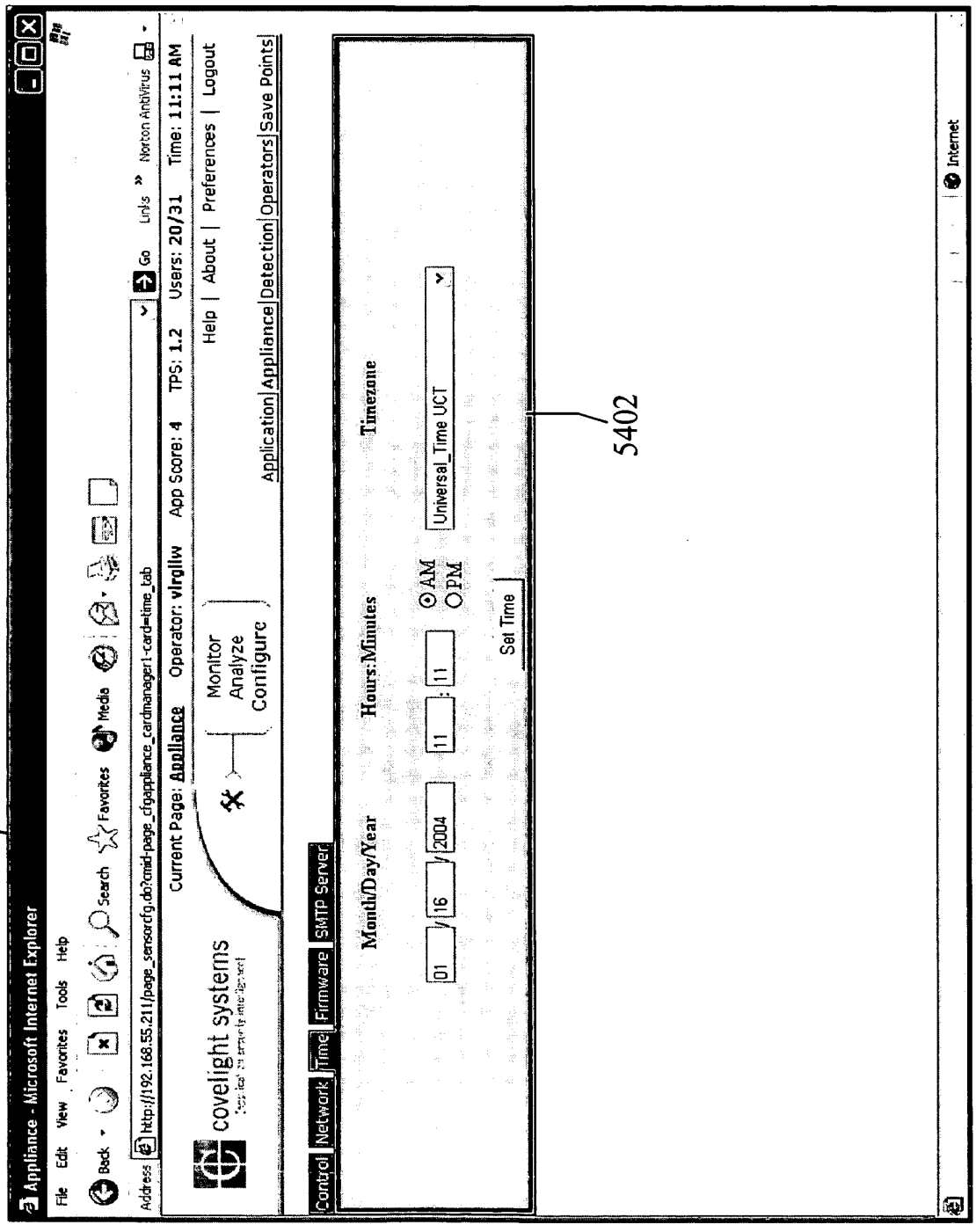
5400
Appliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_sensorcfg.do?cmid=page_cfgappliance_cardmanager1-card=time_tab
Go Links Norton AntiVirus
Current Page: Appliance Operator: virgllw App Score: 4 TPS: 1.2 Users: 20/31 Time: 11:11 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
Control Network Time Firmware SMTP Server
Month/Day/Year
01 / 16 / 2004
Hours:Minutes
11 : 11
AM
PM
Timezone
Universal_Time UCT
Set Time
5402
Internet

FIG. 54

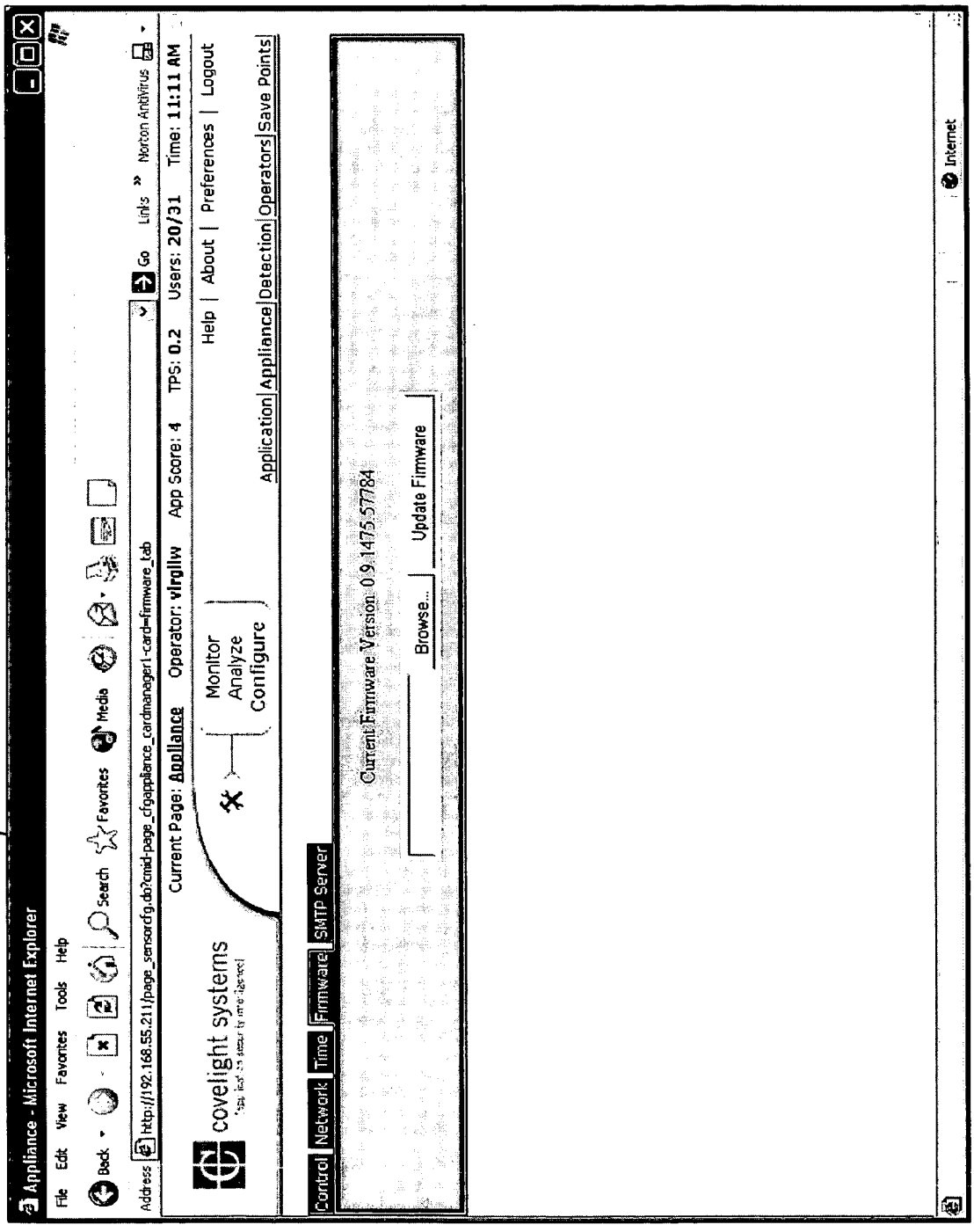
5500
Appliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_sensorcfg.do?cmid=page_cfgappliance_cardmanager1-card=firmware_tab
Go Links Norton AntiVirus
Current Page: Appliance Operator: virgilw App Score: 4 TPS: 0.2 Users: 20/31 Time: 11:11 AM
Help | About | Preferences | Logout
covelight systems
Monitor
Analyze
Configure
Application Appliance Detection Operators Save Points
Control Network Time Firmware SMTP Server
Current Firmware Version: 0.9.1475.57784
Browse...
Update Firmware
Internet

FIG. 55

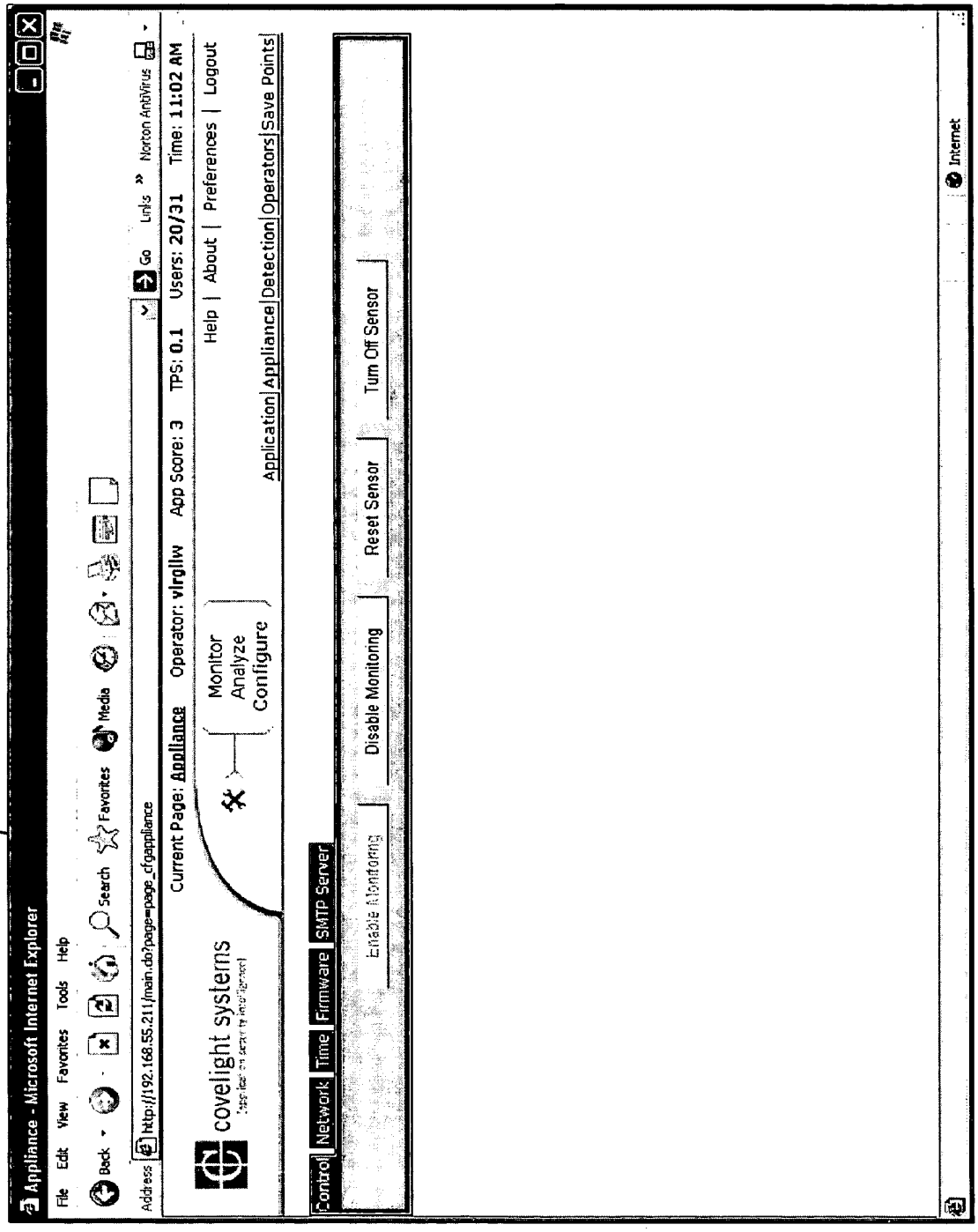
5600
Appliance - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?page=page_cfgappliance
Go Links Norton AntiVirus
Current Page: Appliance Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:02 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
Control Network Time Firmware SMTP Server
Disable Monitoring
Reset Sensor
Turn Off Sensor
Internet

FIG. 56

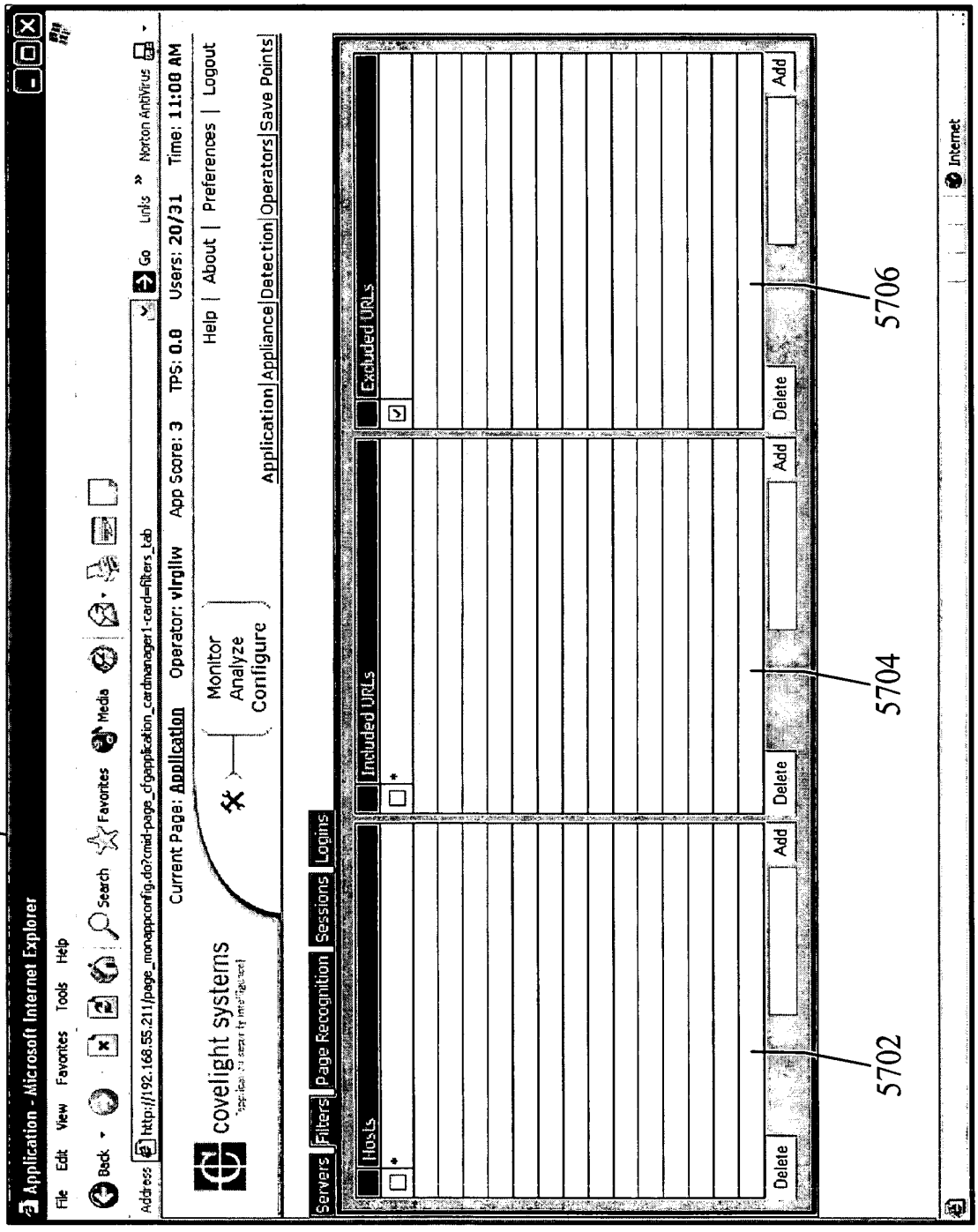
5700
Application - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_monappconfig.do?cmid=page_cfgapplication_cardmanager1-card=filters_tab
Go Links Norton AntiVirus
Current Page: Application Operator: virgilw App Score: 3 TPS: 0.0 Users: 20/31 Time: 11:08 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
Servers Filters Page Recognition Sessions Logins
Hosts
Included URLs
Excluded URLs
Delete
Add
Delete
Add
Delete
Add
5702
5704
5706
Internet

FIG. 57

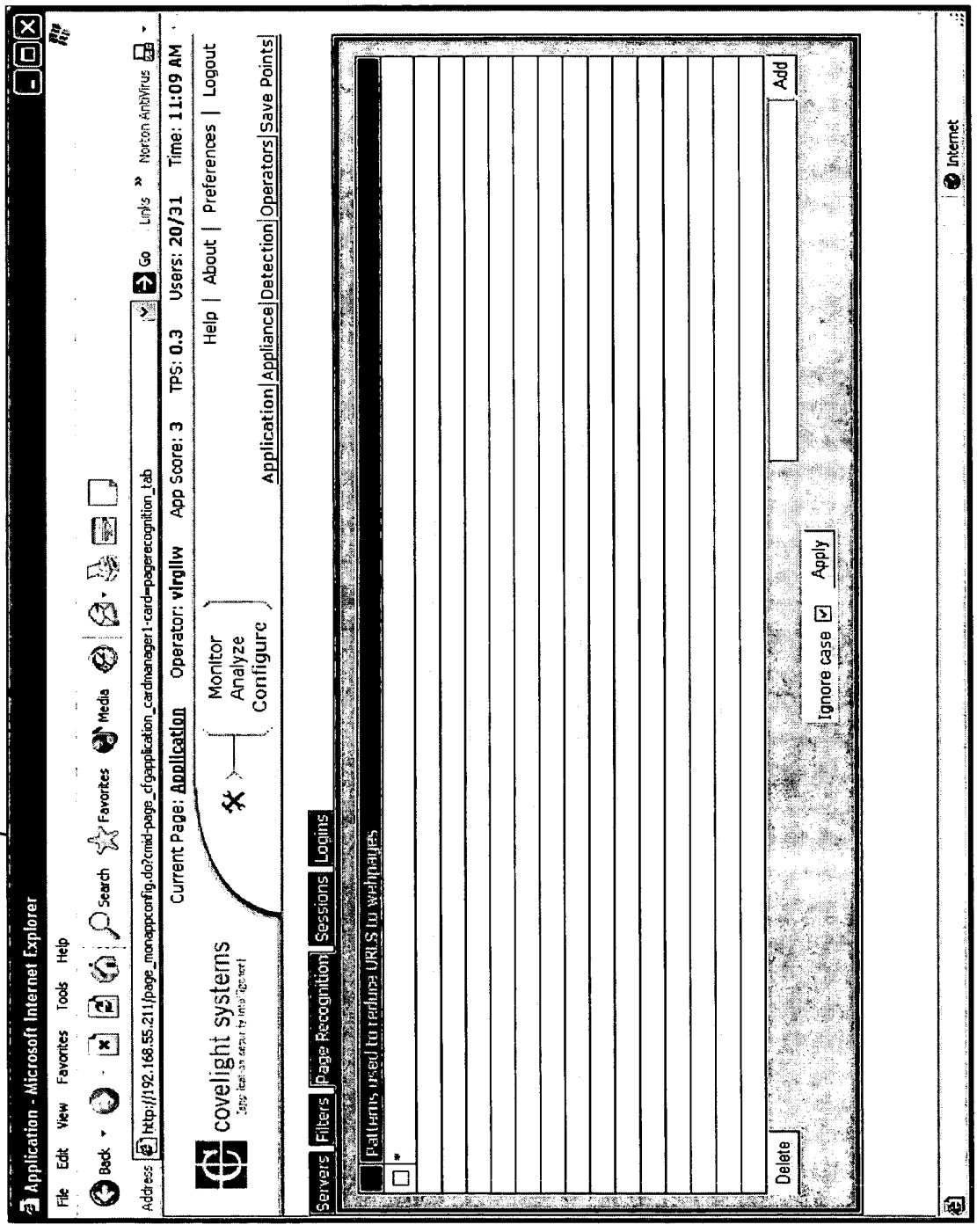
5800
Application - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_monappconfig.do?cmd=page_cfgapplication_cardmanager1-card=pagerecognition_tab
Go Links Norton AntiVirus
Current Page: Application Operator: virgliw App Score: 3 TPS: 0.3 Users: 20/31 Time: 11:09 AM
Help | About | Preferences | Logout
covelight systems
Monitor
Analyze
Configure
Application Appliance Detection Operators Save Points
Servers Filters Page Recognition Sessions Logins
Patterns used to replace URLS in webpages
Delete
Ignore case
Apply
Add
Internet

FIG. 58

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

5900

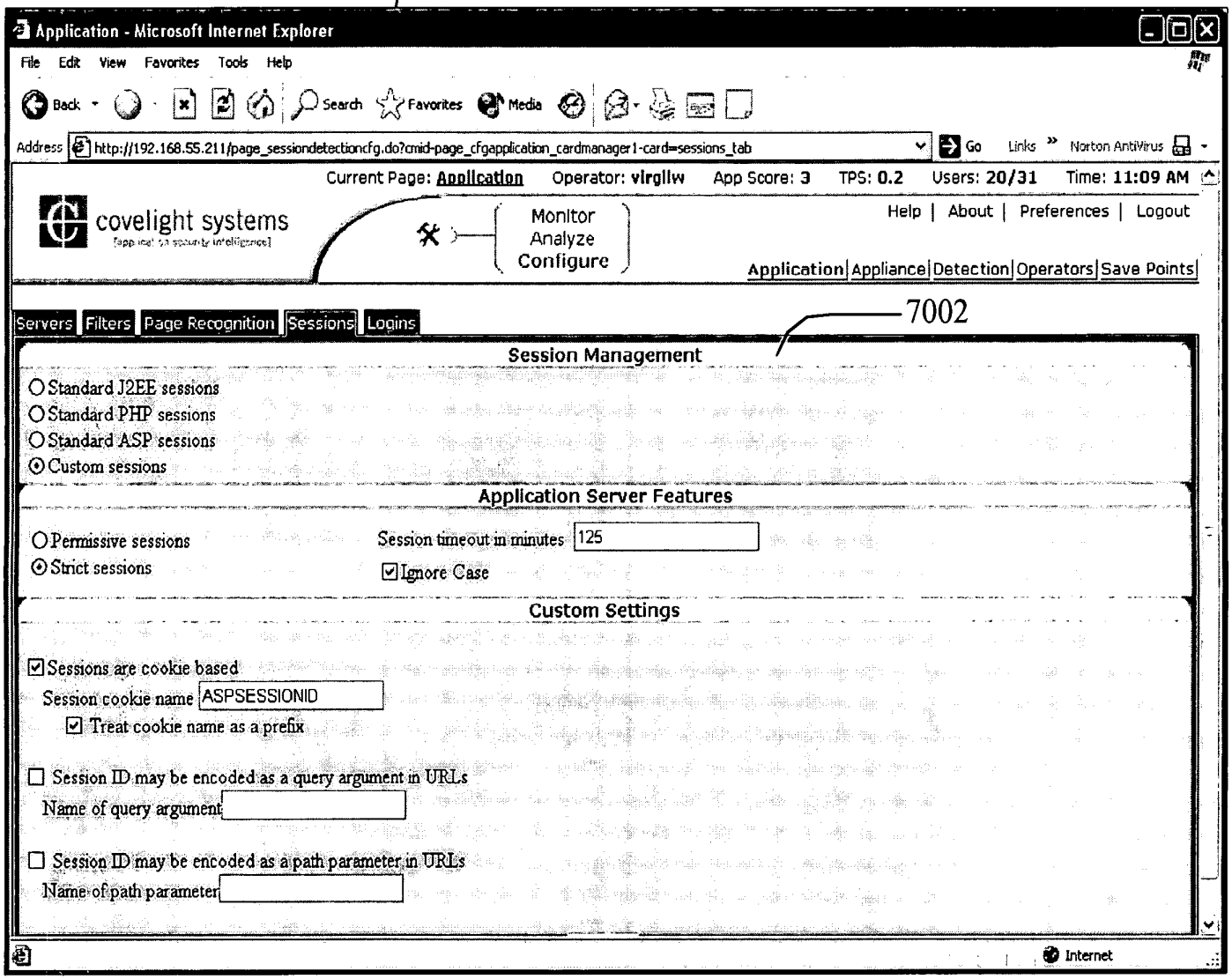

FIG. 59

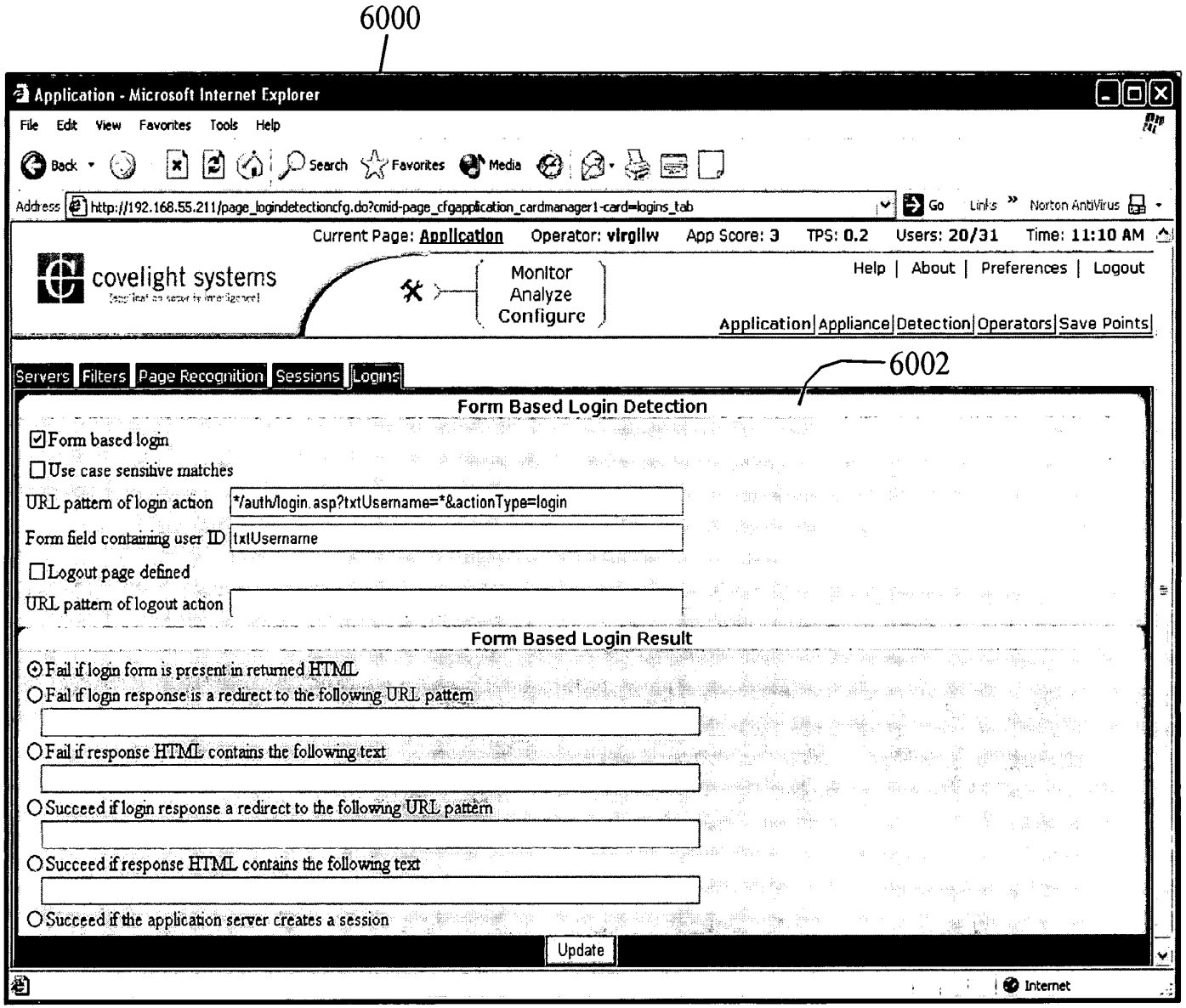

FIG. 60

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

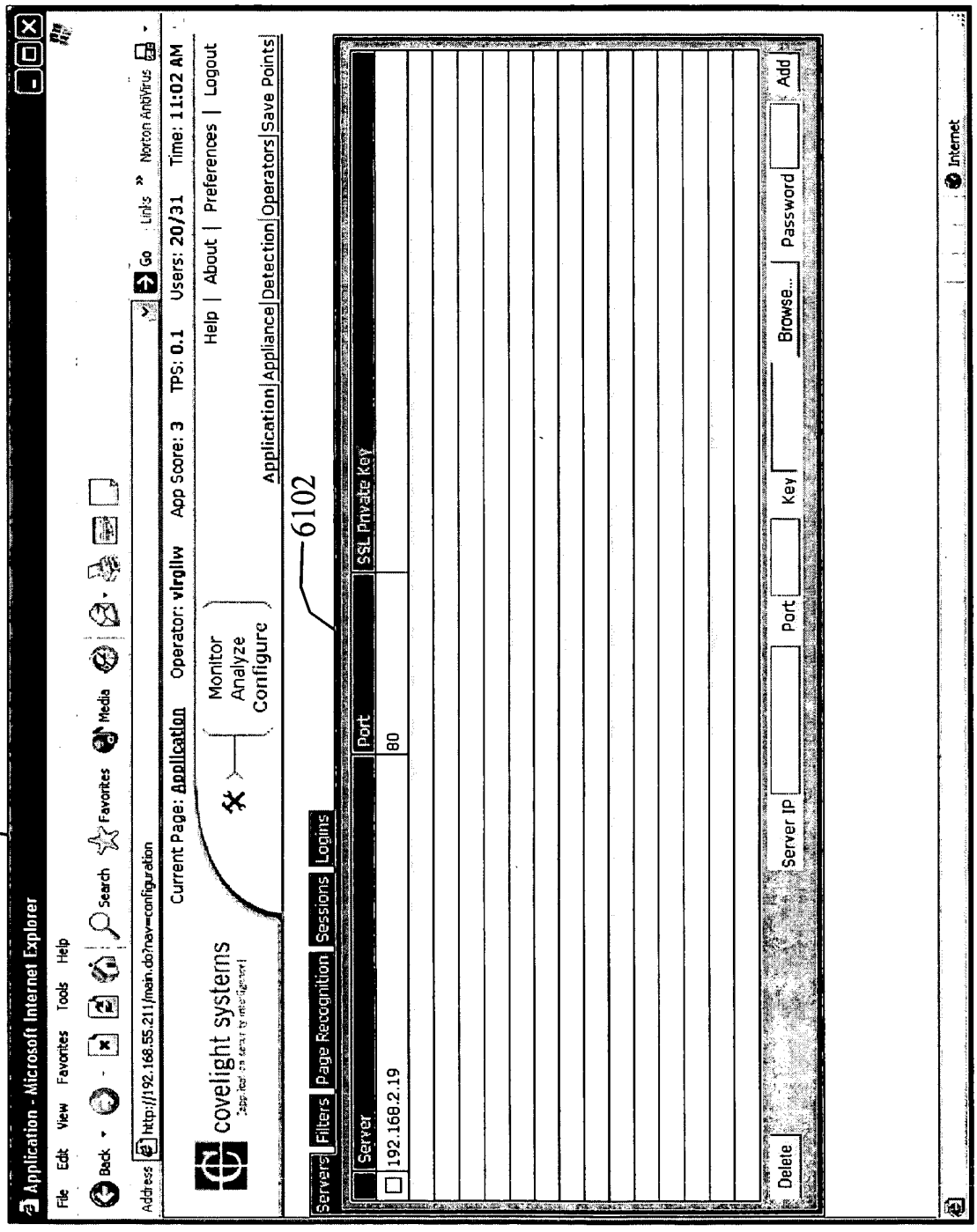
6100
Application - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?nav=configuration
Go Links Norton AntiVirus
Current Page: Application Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:02 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
6102
Servers Filters Page Recognition Sessions Logins
Server
Port
SSL Private Key
192.168.2.19
80
Delete
Server IP
Port
Key
Browse...
Password
Add
Internet

FIG. 61

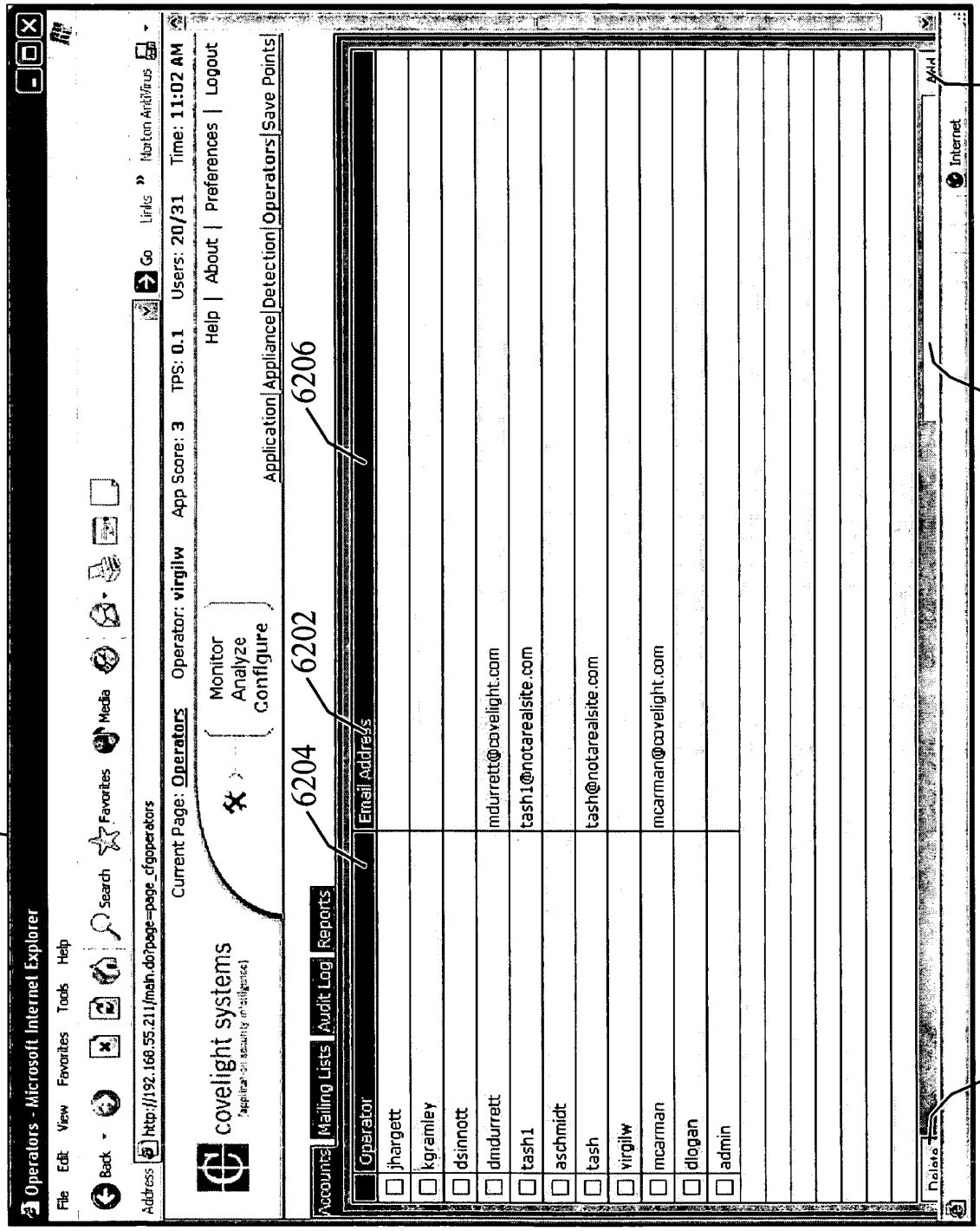
6200
Operators - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?page=page_cfgoperators
Links Norton AntiVirus
Current Page: Operators Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:02 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
6204
6202
6206
Accounts Mailing Lists Audit Log Reports
Operator
Email Address
jhargett
kgramley
dsinnott
dmdurrett mdurrett@covelight.com
tash1 tash1@notarealsite.com
aschmidt
tash tash@notarealsite.com
virgilw
mcarman mcarman@covelight.com
dlogan
admin
Delete
Internet
6208
6212
6210

FIG. 62

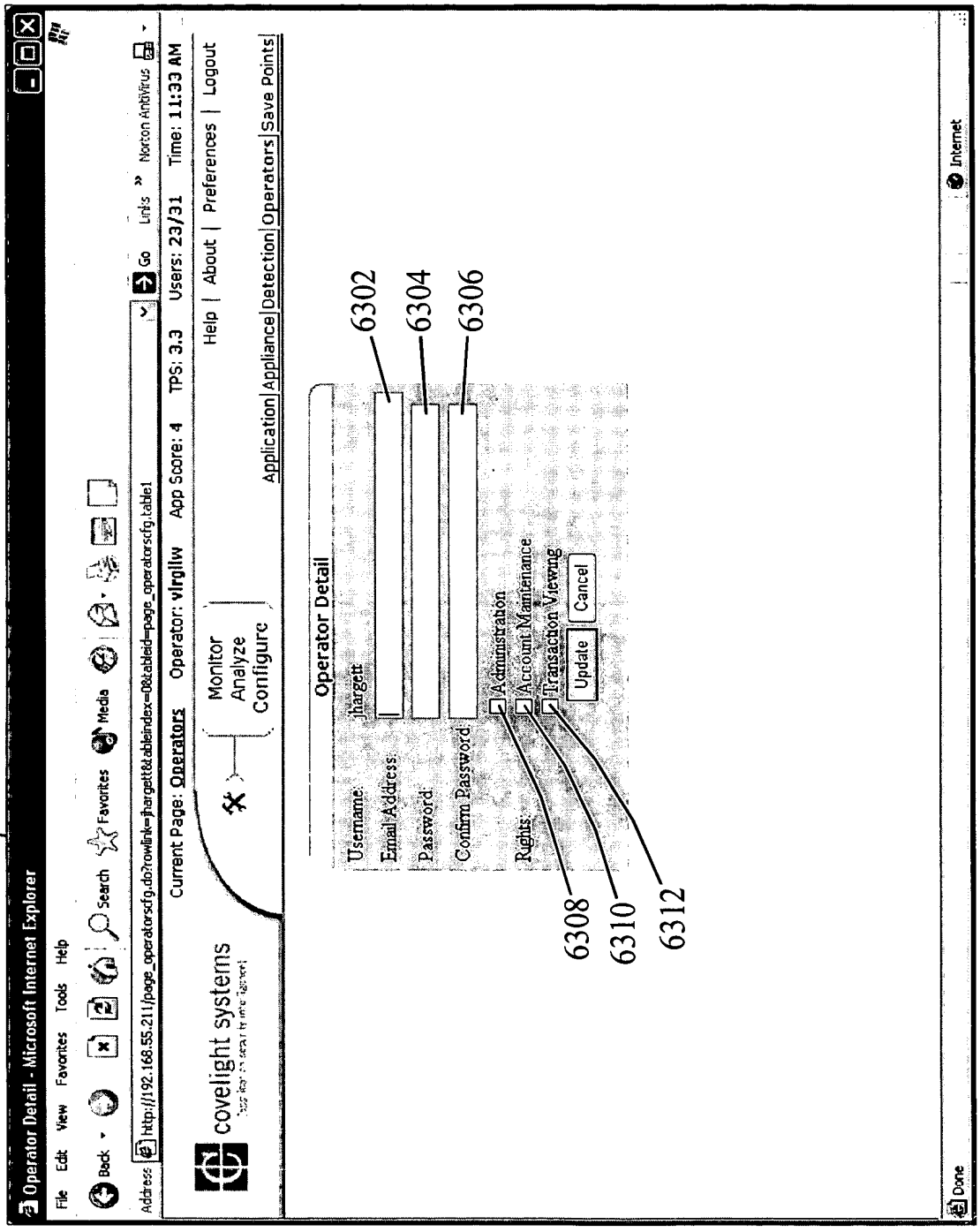
6300
Operator Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_operatorscfg.do?rowlink=jhargett&tableindex=08&tableid=page_operatorscfg.table1
Go Links Norton AntiVirus
Current Page: Operators Operator: virgilw App Score: 4 TPS: 3.3 Users: 23/31 Time: 11:33 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
Operator Detail
Username: jhargett
Email Address:
Password:
Confirm Password:
Rights:
Administration
Account Maintenance
Transaction Viewing
Update
Cancel
6302
6304
6306
6308
6310
6312
Done
Internet

FIG. 63

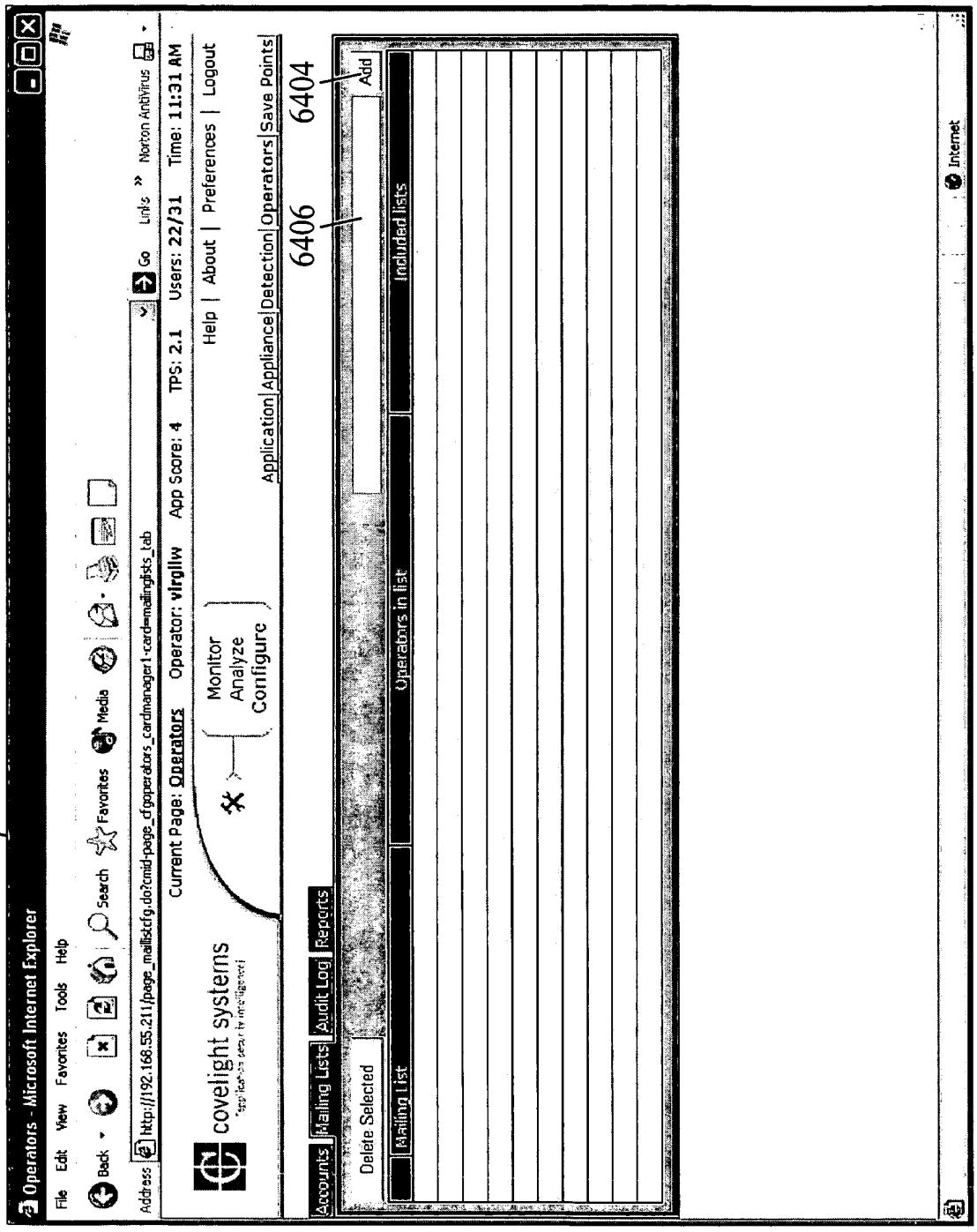
6400
Operators - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_mailinglistcfg.do?cmid=page_cfgoperators_cardmanager1-card=mailinglists_tab
Go Links Norton AntiVirus
Current Page: Operators Operator: virgilw App Score: 4 TPS: 2.1 Users: 22/31 Time: 11:31 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
6406 6404
Accounts Mailing Lists Audit Log Reports
Delete Selected
Add
Mailing List
Operators in list
Included lists
Internet

FIG. 64

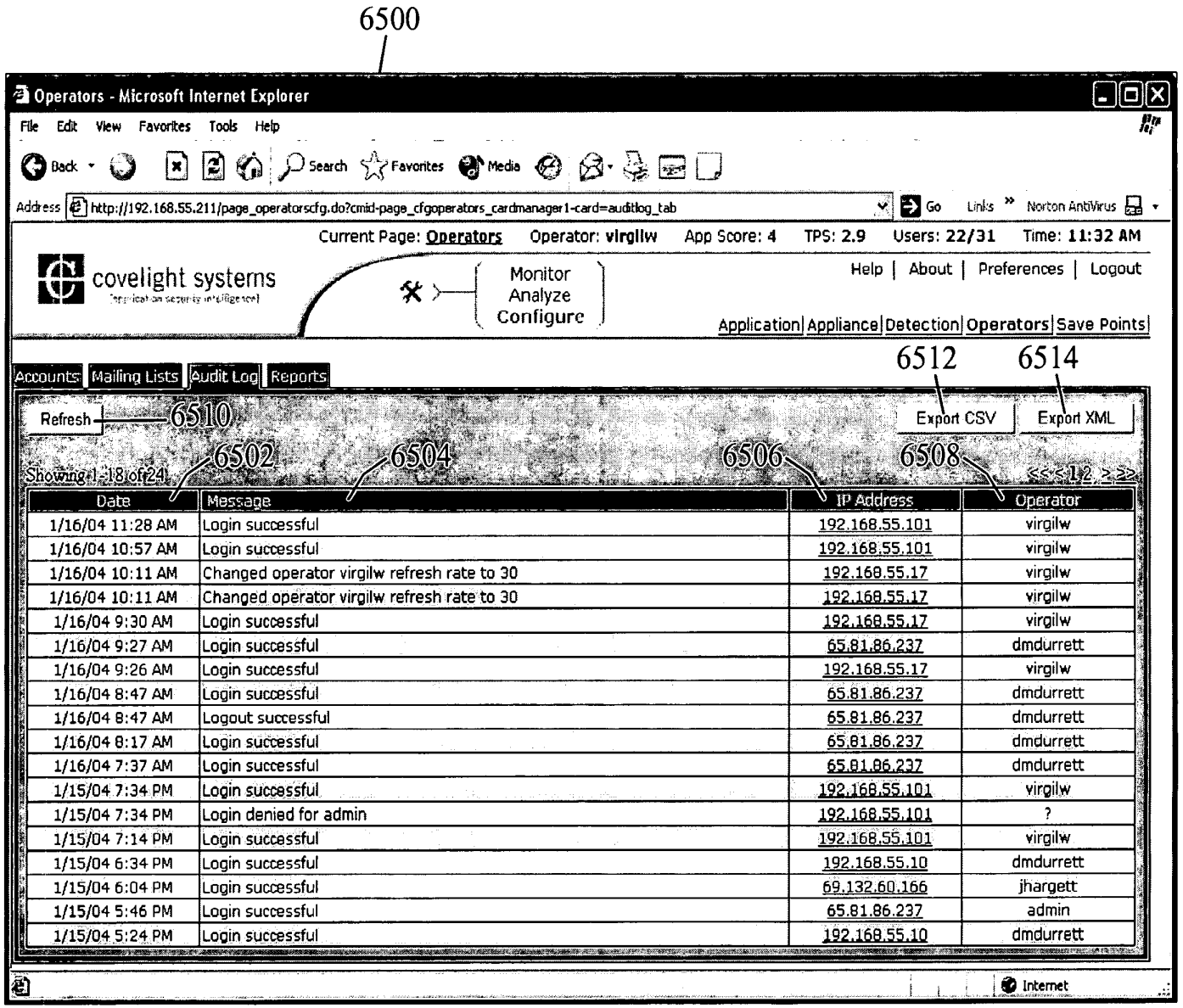

FIG. 65

REPLACEMENT SHEET
Title: METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR MONITORING A SERVER APPLICATION
Applicant(s): Motsinger et al.
Atty. Docket No.: 1503/6

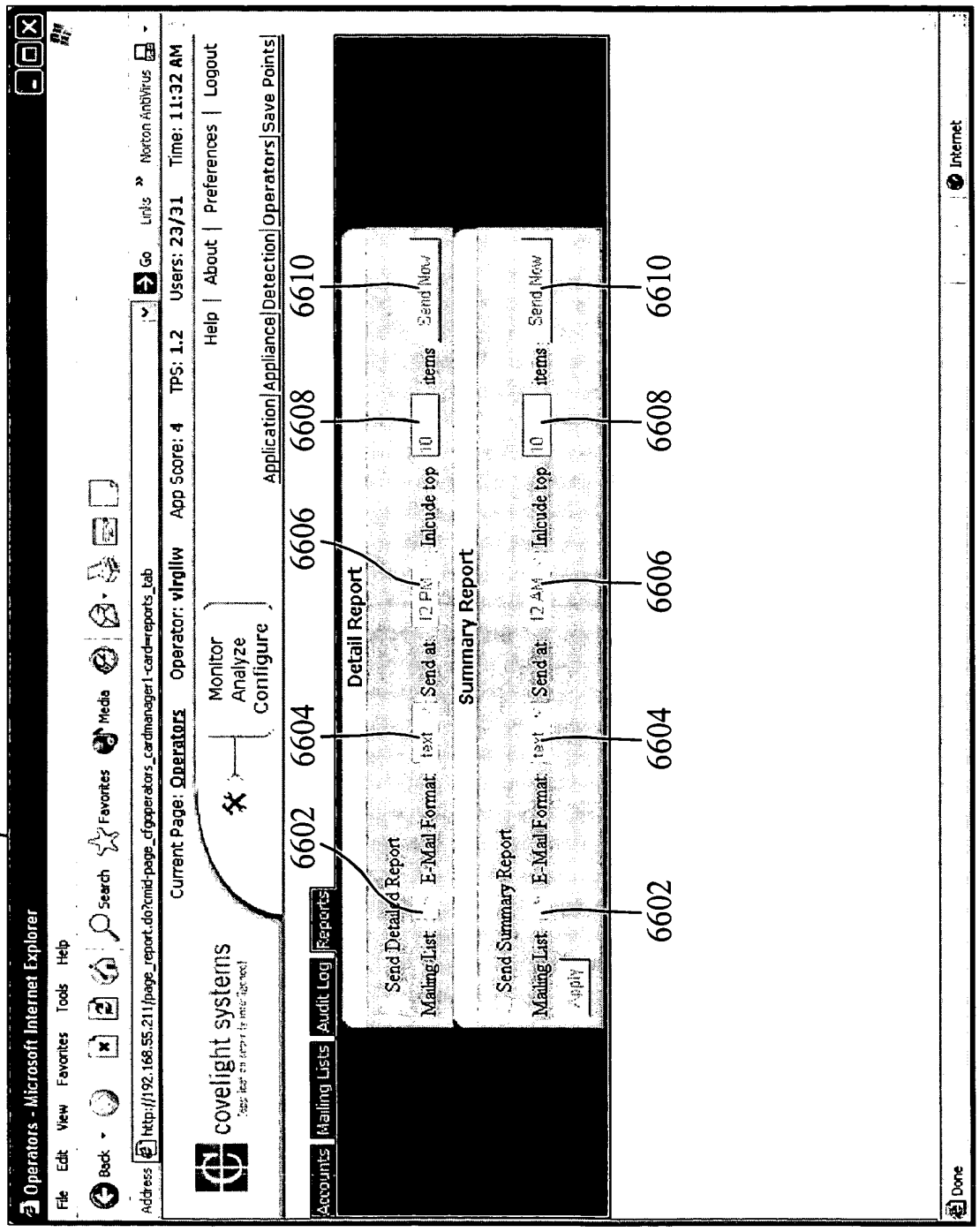
6600
Operators - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.55.211/page_report.do?cmid=page_cfgoperators_cardmanager1-card=reports_tab
Current Page: Operators Operator: virgilw App Score: 4 TPS: 1.2 Users: 23/31 Time: 11:32 AM
Help | About | Preferences | Logout
covelight systems
Monitor
Analyze
Configure
Application Appliance Detection Operators Save Points
Accounts Mailing Lists Audit Log Reports
6602 6604 6606 6608 6610
Detail Report
Send Detailed Report
Mailing List E-Mail Format: text Send at: 12 PM Include top 10 items Send Now
Summary Report
Send Summary Report
Mailing List E-Mail Format: text Send at: 12 AM Include top 10 items Send Now
Apply
6602 6604 6606 6608 6610
Done
Internet

FIG. 66

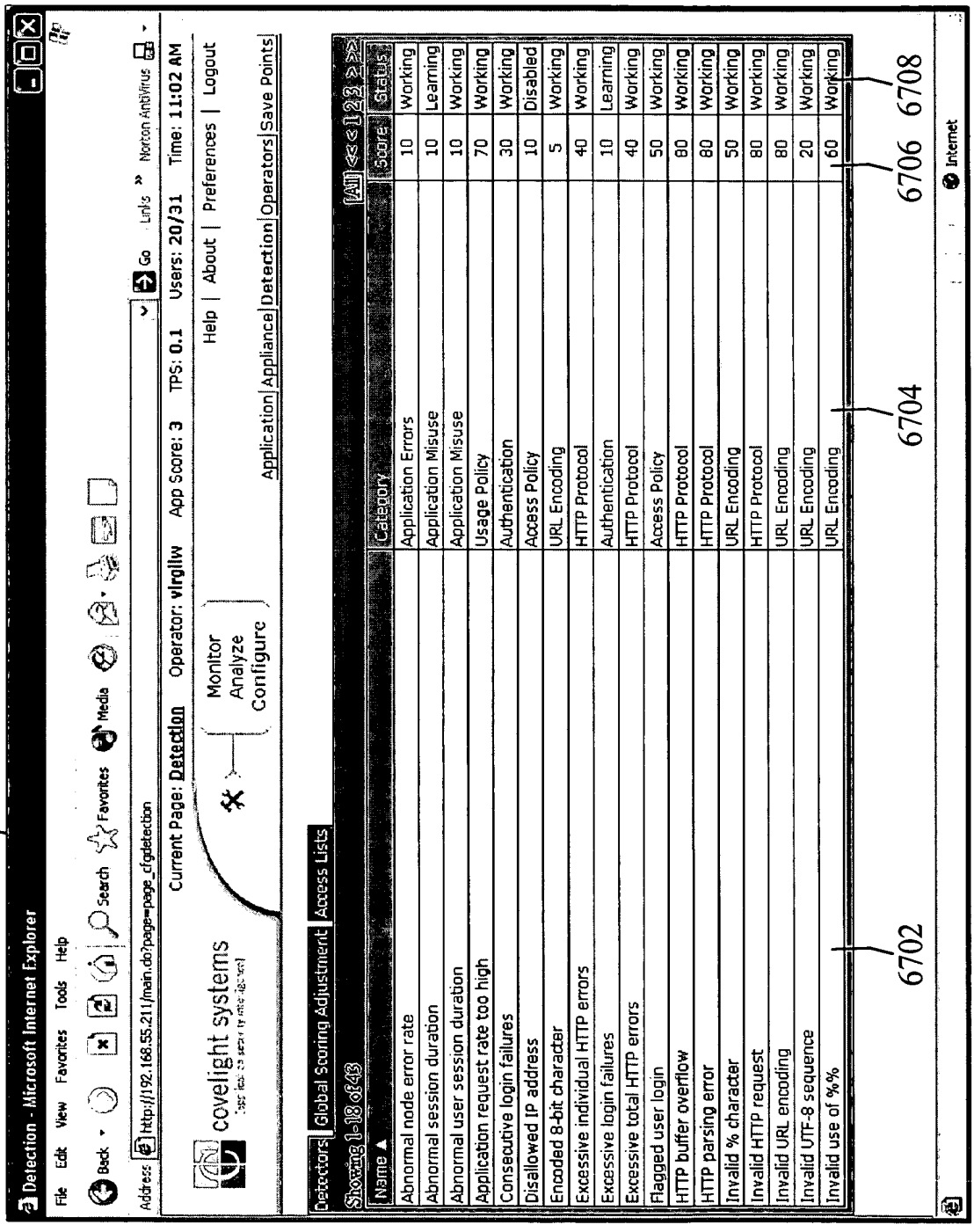
6700
Detection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/main.do?page=page_cfgdetection
Go Links Norton AntiVirus
Current Page: Detection Operator: virgilw App Score: 3 TPS: 0.1 Users: 20/31 Time: 11:02 AM
Help | About | Preferences | Logout
covelight systems
Monitor
Analyze
Configure
Application Appliance Detection Operators Save Points
Detectors Global Scoring Adjustment Access Lists
Showing 1-18 of 18
[All] << < 1 2 3 > >>
Name
Category
Score
Status
Abnormal node error rate | Application Errors | 10 | Working
Abnormal session duration | Application Misuse | 10 | Learning
Abnormal user session duration | Application Misuse | 10 | Working
Application request rate too high | Usage Policy | 70 | Working
Consecutive login failures | Authentication | 30 | Working
Disallowed IP address | Access Policy | 10 | Disabled
Encoded 8-bit character | URL Encoding | 5 | Working
Excessive individual HTTP errors | HTTP Protocol | 40 | Working
Excessive login failures | Authentication | 10 | Learning
Excessive total HTTP errors | HTTP Protocol | 40 | Working
Flagged user login | Access Policy | 50 | Working
HTTP buffer overflow | HTTP Protocol | 80 | Working
HTTP parsing error | HTTP Protocol | 80 | Working
Invalid % character | URL Encoding | 50 | Working
Invalid HTTP request | HTTP Protocol | 80 | Working
Invalid URL encoding | URL Encoding | 80 | Working
Invalid UTF-8 sequence | URL Encoding | 20 | Working
Invalid use of %% | URL Encoding | 60 | Working
6702
6704
6706
6708
Internet

FIG. 67

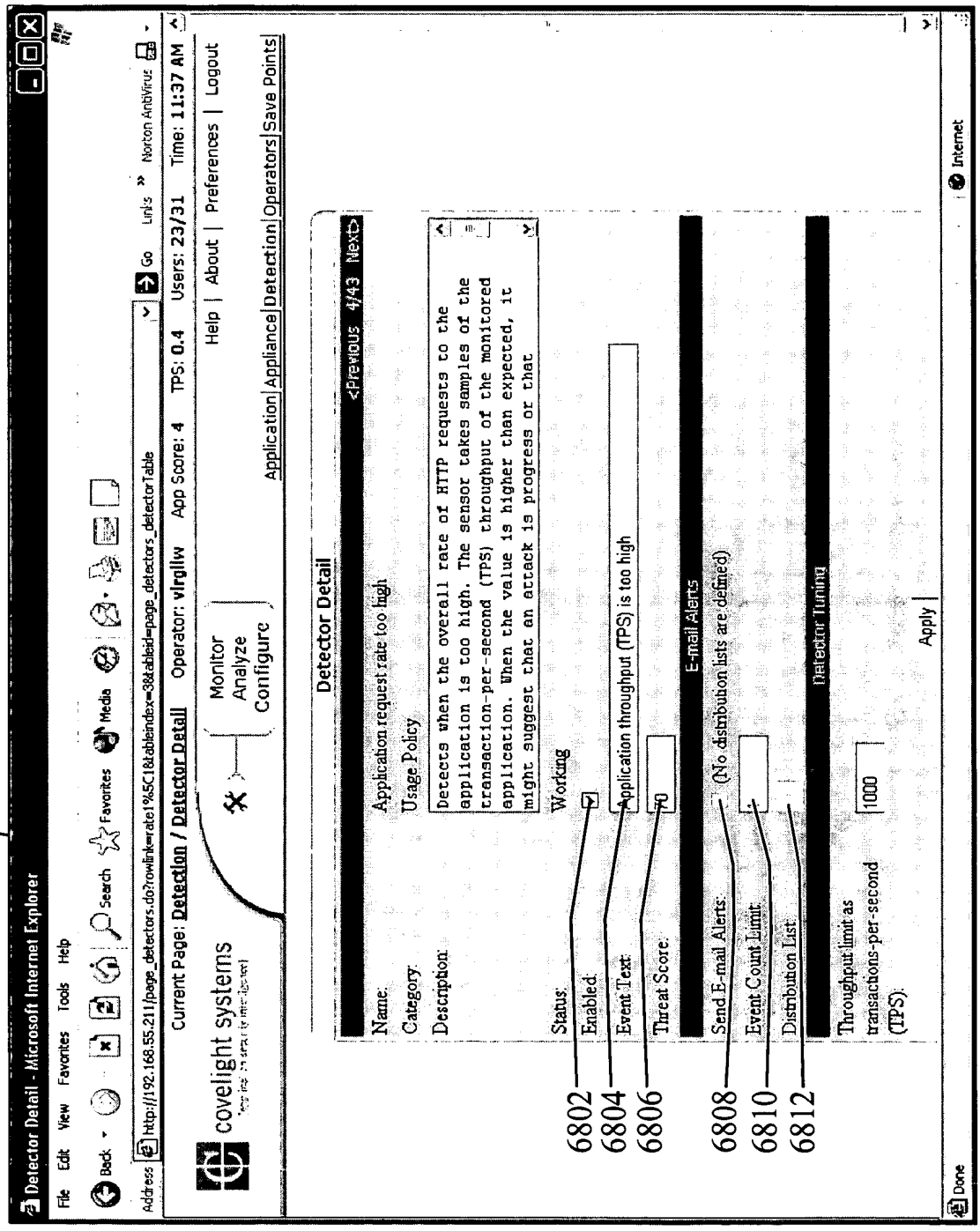
6800
Detector Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.55.211/page_detectors.do?rowlink=rate1%5C1&tableindex=3&tableid=page_detectors_detectorTable
Current Page: Detection / Detector Detail Operator: virgilw App Score: 4 TPS: 0.4 Users: 23/31 Time: 11:37 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
Detector Detail
<Previous 4/43 Next>
Name: Application request rate too high
Category: Usage Policy
Description: Detects when the overall rate of HTTP requests to the application is too high. The sensor takes samples of the transaction-per-second (TPS) throughput of the monitored application. When the value is higher than expected, it might suggest that an attack is progress or that
Status: Working
Enabled:
Event Text: Application throughput (TPS) is too high
Threat Score: 70
E-mail Alerts
Send E-mail Alerts: (No distribution lists are defined)
Event Count Limit:
Distribution List:
Detector Tuning
Throughput limit as transactions-per-second (TPS): 1000
Apply
6802
6804
6806
6808
6810
6812
Done
Internet

FIG. 68

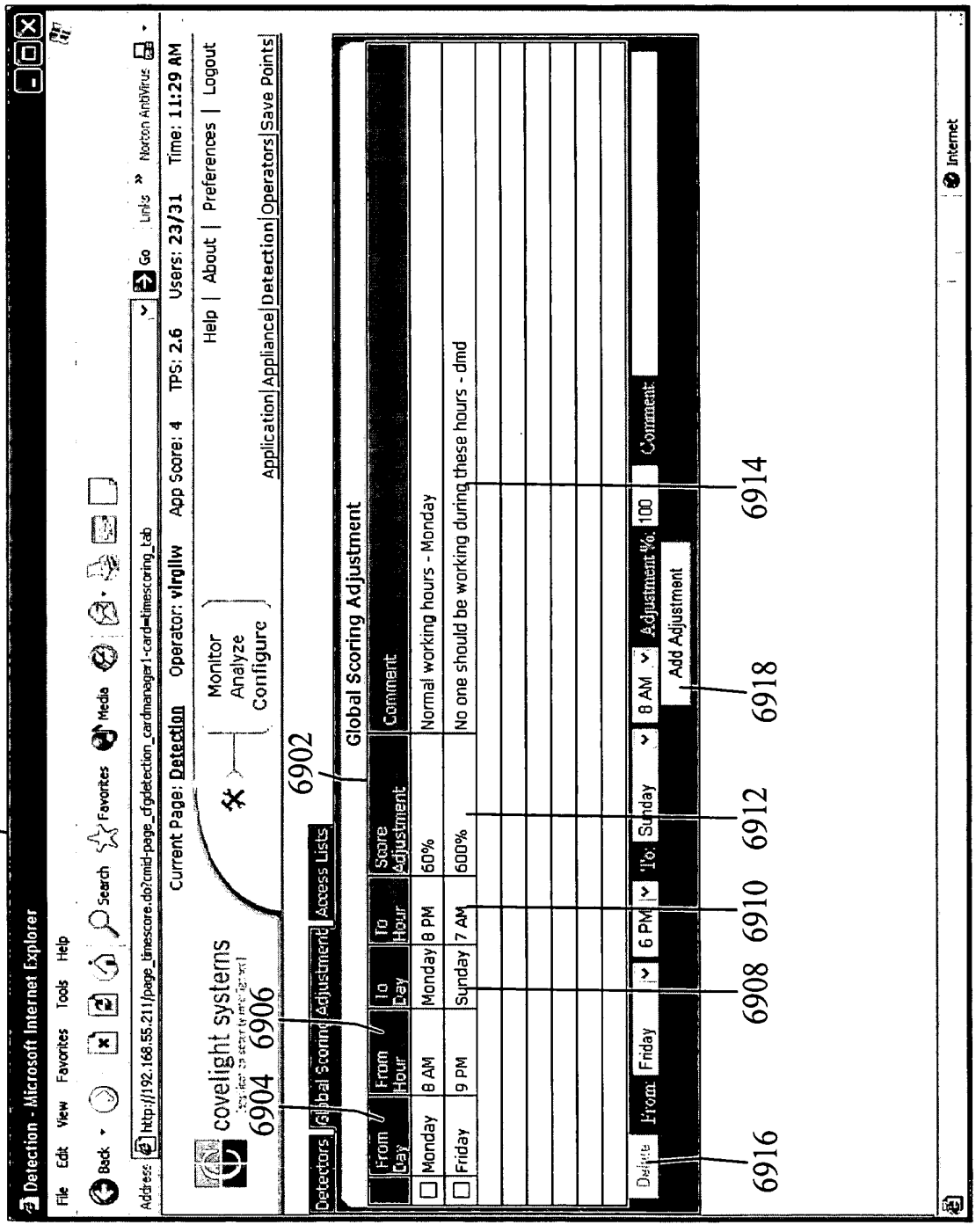
6900
Detection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_timescore.do?cmid=page_dfgdetection_cardmanager1-card=timescoring_tab
Go Links Norton AntiVirus
Current Page: Detection Operator: virgilw App Score: 4 TPS: 2.6 Users: 23/31 Time: 11:29 AM
covelight systems
Monitor
Analyze
Configure
Help | About | Preferences | Logout
Application Appliance Detection Operators Save Points
6902
Detectors Global Scoring Adjustment Access Lists
6904 6906
Global Scoring Adjustment
From Day
From Hour
To Day
To Hour
Score Adjustment
Comment
Monday 8 AM Monday 8 PM 60% Normal working hours - Monday
Friday 9 PM Sunday 7 AM 600% No one should be working during these hours - dmd
Delete
From: Friday 6 PM To: Sunday 8 AM Adjustment %: 100 Comment:
Add Adjustment
6916 6908 6910 6912 6918 6914
Internet

FIG. 69

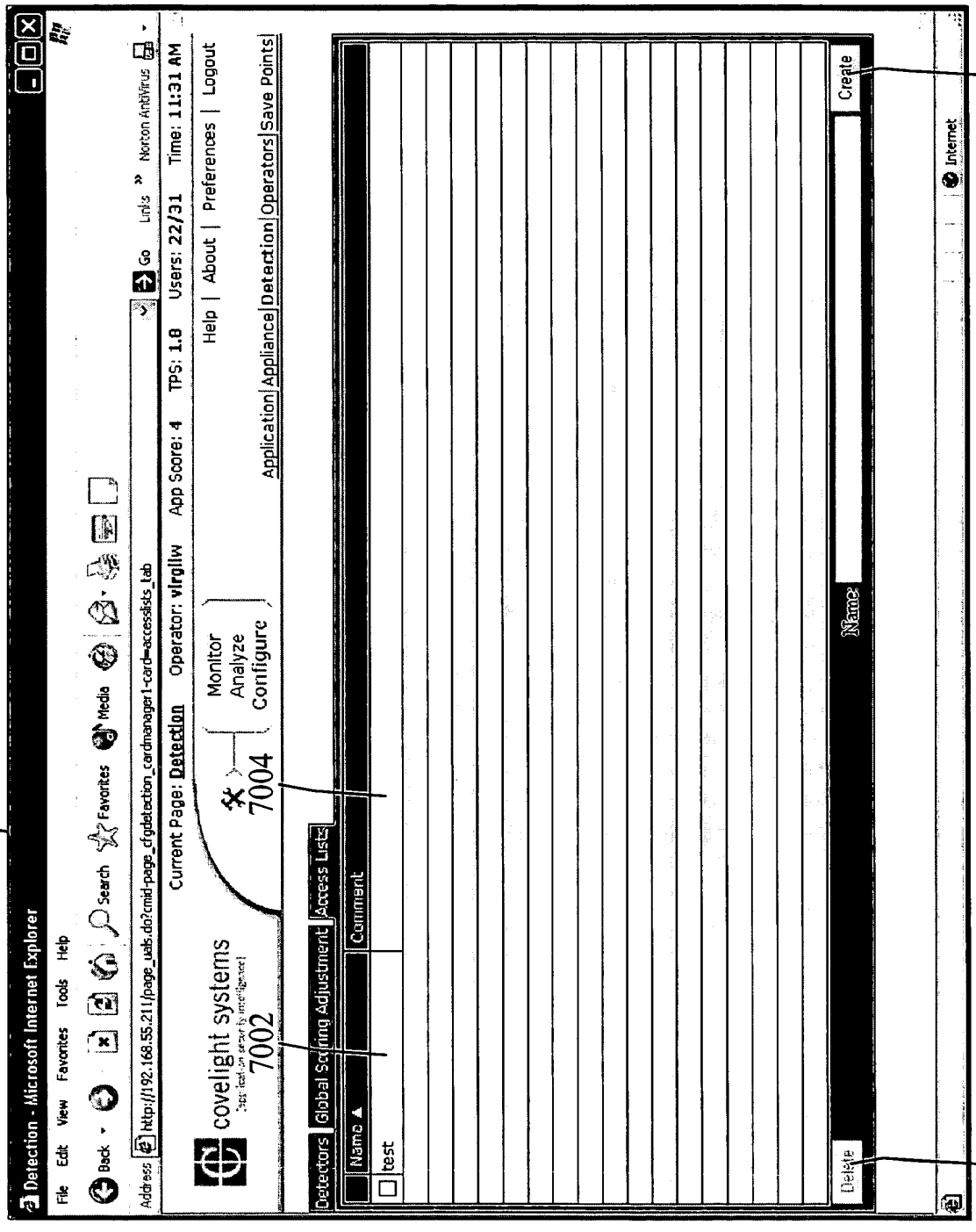
7000
Detection - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.55.211/page_uab.do?cmid=page_cfgdetection_cardmanager1-card=accesslists_tab
Go Links Norton AntiVirus
Current Page: Detection Operator: virgilw App Score: 4 TPS: 1.8 Users: 22/31 Time: 11:31 AM
Help | About | Preferences | Logout
covelight systems
7002
Monitor
Analyze
Configure
7004
Application Appliance Detection Operators Save Points
Detectors Global Scoring Adjustment Access Lists
Name
Comment
test
Delete
Name
Create
7006
7008
Internet

FIG. 70

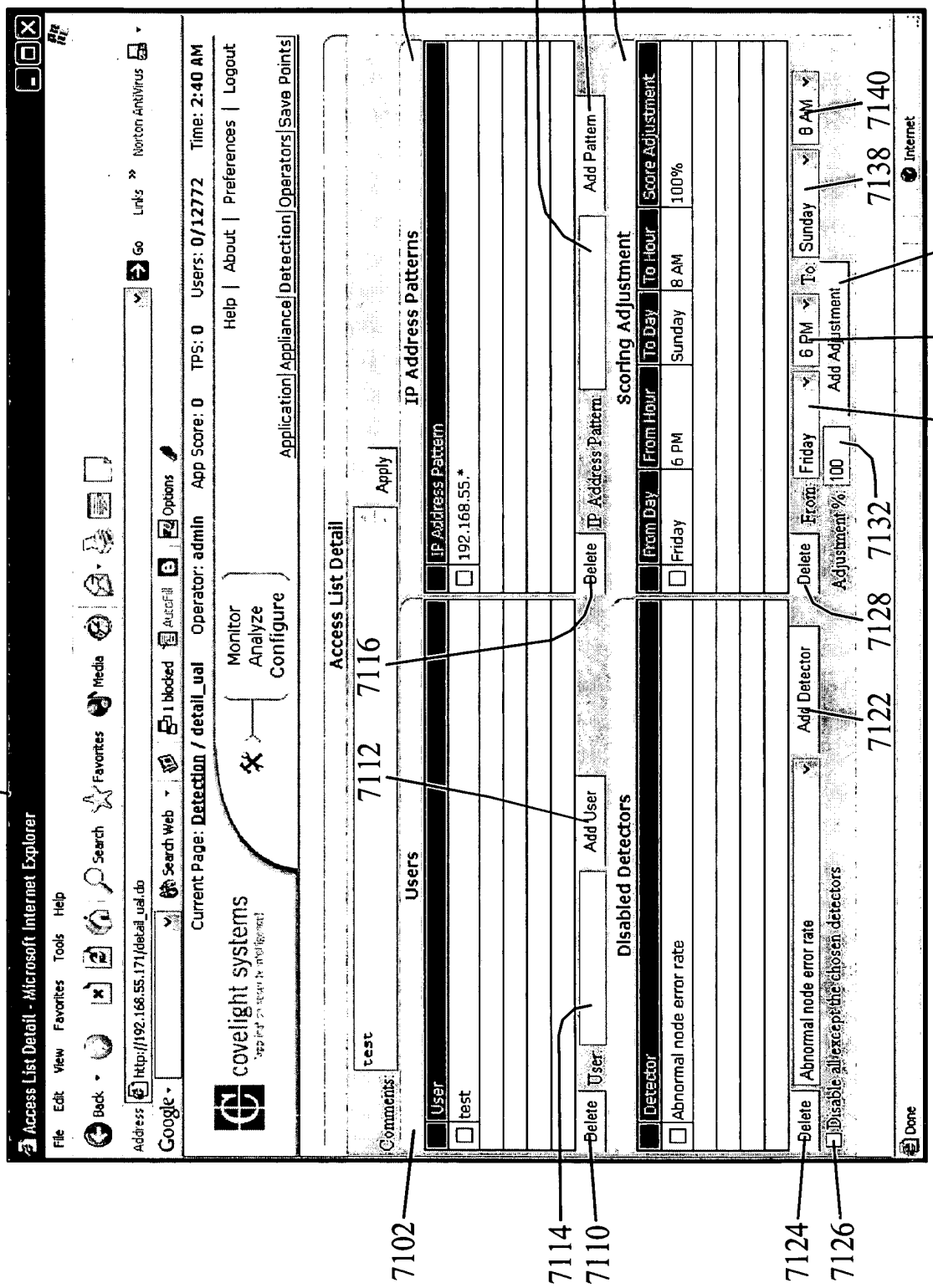
7100
Access List Detail - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.55.171/detail_ual.do
Current Page: Detection / detail_ual Operator: admin App Score: 0 TPS: 0 Users: 0/12772 Time: 2:40 AM
Help | About | Preferences | Logout
covelight systems
Monitor
Analyze
Configure
Application Appliance Detection Operators Save Points
Access List Detail
Comments: test
Apply
Users
User
test
Delete User
Add User
Disabled Detectors
Detector
Abnormal node error rate
Delete Abnormal node error rate
Add Detector
Disable all except the chosen detectors
IP Address Patterns
IP Address Pattern
192.168.55.*
Delete IP Address Pattern
Add Pattern
Scoring Adjustment
From Day From Hour To Day To Hour Score Adjustment
Friday 6 PM Sunday 8 AM 100%
Delete From: Friday 6 PM To: Sunday 8 AM
Adjustment %: 100
Add Adjustment
Done
Internet
7102
7104
7108
7110
7112
7114
7116
7118
7120
7122
7124
7126
7128
7130
7132
7134
7136
7138
7140

FIG. 71